Pour aller plus loin quelques sites :

- **Sur le site de Tails,** il y a une page de documentation très bien faite **:** https://tails.boum.org/doc/index.fr.html
- Le **guide d'autodéfense numérique (référence en cas de doute de ce que pourrait dire d'autres sites)**, par ici : https://guide.boum.org/ → Ce guide a été fait à destination des militant.es, il pose à la fois les problématiques politiques ainsi que des réponses techniques et des tutoriels à faire sur Tails et sur debian.
- ***Guide de survie en protection numérique à l'usage des militant·es***, brochure disponible sur infokiosques.net
- Pages de riseup sur la sécurité (humaine, matériel, réseau), tout n'y est pas traduit : https://riseup.net/fr/security
- Security-in-a-box est un guide de sécurité numérique destiné aux activistes et défenseureuses des droits humains dans le monde : https://securityinabox.org/en/

Listes de logiciels et de services alternatifs

- Une liste de sites militants qui font de l'hébergement, des vpn, des adresses mail ou tout un tas d'autres services basés pour faire de la sécurité informatique et la non récolte des données (riseup) : https://riseup.net/fr/security/resources/radical-servers
- Pas mal d'astuces pour des alternatives aux services propriétaires : https://technopolice.be/autodefense-numerique/
- Liste logiciels libres et sites alternatifs (pour trouver des alternatives aux multinationales du numérique) : https://prism-break.org/fr/ ou https://www.chatons.org/ ou encore https://framalibre.org/alternatives

Site d'info et d'analyse

- Informations sur les lois de surveillance numérique : https://www.laquadrature.net/

Outils pédagogiques

- Outil visuel pour savoir qui nous traque sur un certain nombre de sites : https://trackography.org/ Donnés numériques récoltés sur 6 mois : https://www.digitale-gesellschaft.ch/vds-suisse/index_fr.html Outils pédagogiques sur ce qu'on peut récolter à partir de notre navigation : https://coveryourtracks.eff.org/ (anglais)
- Au sujet des données laissées sur internet : https://myshadow.org/fr

Autres

- Si tu veux payer des choses de manière anonyme (bitcoin et autres). Un article par ici: https://rebellyon.info/Comment-payer-de-maniere-anonyme-sur-le.html
- Faire sa propre carte interactive : https://umap.openstreetmap.fr/fr/
- Utiliser la plateforme de communication vocale Mumble sur Tails (anglais) : https://autonomia.digital/2019/10/09/tails-mumble.html

Contact : des questions / critiques / remarques ? souslaplage@riseup.net
Brochure à vocation d'être mise à jour, retrouvable sur **infokiosques.net**

TuTORiel Tails



Septembre 2022 version Tails 5.4

Table des matières

Quelques explications.....4
▪ *Notion de modèle de menace*.....5
I) Bases pour utiliser Tails.....6
Préalable.....6
Comment utiliser ce tuto ?.....6
Installation.....7
▪ *[SOLUTION 1] Installation à partir d'une autre clé Tails*.....7
▪ *[SOLUTION 2] Installation par téléchargement*.....7
> Booter sur ta clé Tails.....7
▪ *Réglage du bios / programme UEFI*.....9
▪ *Cas des windows 8 ou 10 (si c'est la première fois que tu démarres sur un autre système d'exploitation)*.....10
> Démarrer sur Tails.....11
▪ *Pas d'onglet wifi ?*.....13
> Configurer la persistance / stockage de données sur la clé Tails.....13
▪ *Changer sa phrase de passe*.....14
▪ *J'ai oublié ma phrase de passe*.....14
▪ *Configurer une bonne phrase de passe*.....15
> Installer une clé Tails (à partir d'une clé Tails).....16
▪ *Éviter d'avoir une clé vérolée*.....16
> Mettre à jour une clé Tails.....16
II) Pour aller plus loin : quelques trucs et astuces supplémentaires.....18
> Supprimer vraiment des données d'une clé usb.....18
> Comment créer un disque dur ou une clé usb chiffrée (ouvrable sur des linux).....18
> Chiffrer un fichier / un document par une phrase de passe – ou par une clé publique.....19
▪ *Sur un fichier de manière générale*.....19
▪ *Sur un document Libre Office*.....19
> S'ajouter des droits d'administrateurices.....19
> MAT2 - supprimer les métadonnées sur des fichiers.....20
▪ *Cas du pdf :*.....20
> Coffre fort à mot de passe (KeePassXC).....21
▪ *Rendre persistent les paramétrages de KeepassXC*.....22
▪ *Utiliser les paramètres de remplissage automatique de KeePassXC*.....22
> Téléchargement / téléversement et le dossier Tor browser.....23
▪ *Peu de RAM ou téléchargement de gros fichiers*.....23
▪ *Format de fichier HTML*.....23
▪ *Document téléchargé et vérifications*.....23
> Installer des logiciels additionnels.....24
> Chiffrer ses mails (avec Thunderbird).....25
▪ *Quelques explications de OpenPGP*.....25
▪ *Configurer un compte de messagerie électronique*.....26
▪ *Tableau récapitulatif des différences entre pop et imap*.....26
▪ *Configuration de la clé privée OpenPGP dans thunderbird.*.....27
▪ *Afficher et gérer les paramètres des clés / vérification de l'empreinte numérique*.....27
▪ *Envoyer sa clé publique / une clé publique d'autres personnes*.....28
▪ *Récupérer une clé publique / envoyer un message chiffré*.....28
▪ *Mettre les serveurs .onion de riseup dans Thunderbird*.....29
> Tor.....29
▪ *Qu'est-ce que Tor?*.....29
▪ *Qu'est-ce que HTTPS ?*.....30

va essayer ici de récupérer. **Surtout n'importe pas une nouvelle clé publique ou ne créé pas une nouvelle clé privée** avant cette démarche sinon ça va écraser cette sauvegarde.

Pour cela, on va dans `Emplacements ▸ Dossier Personnel ▸ [taper CTRL+h pour afficher les fichiers cachés] ▸ .thinderbird ▸ Profil.default`

Pour les clés publiques : Tu trouveras les fichiers pubring.gpg ainsi que pubring.gpg.old. Si tu sélectionne le fichier, tu peux voir son poids en bas à droite. Si pubring.gpg est à 0 octet, et que pubring.gpg.old a un poids plus important, t'as une chance de tout récupérer. Il suffit de supprimer pubring.gpg et de renommer pubring.gpg.old en pubring.gpg.
Pour les clés privés : Même principe avec secring.gpg et secring.gpg.old. Ensuite tu redémarre Thunderbird. Pour limiter le risque de tout perdre, pense à faire des sauvegardes.

> Pense à faire des sauvegardes ! Très important !!!

Une clé Tails ça se perd facilement, ça se fait piquer et les clés usb ont une durée de vie bien moindre qu'un disque dur (surtout les premiers prix). Si t'y mets des données importantes, pense à y faire des sauvegardes régulièrement. Pour **sauvegarder ton dossier persistant,** c'est simple, tu peux copier sur une autre clé chiffrée tes documents. Si tu veux sauvegarder toutes tes configurations enregistrées dans la persistance (thunderbird, pidgin, mots de passe wifi…) pour retrouver ta clé Tails à l'identique, un outil simple d'usage est à disposition.

Créer un nouveau Tails pour enregistrer votre sauvegarde

1) Installez Tails sur une nouvelle clé USB sur laquelle vous voulez créer votre Tails de sauvegarde. Assurez-vous que cette nouvelle clé USB est au moins de capacité égale à celle de votre clé USB Tails actuelle. Nous vous recommandons de faire votre Tails de sauvegarde sur une clé USB qui a une apparence différente de votre clé USB Tails actuelle pour éviter d'utiliser votre Tails de sauvegarde par erreur. Éteignez et débranchez votre clé USB Tails actuelle.

2) Redémarrez sur votre Tails de sauvegarde et créez un stockage persistant sur celui-ci - Nous vous recommandons d'utiliser la même phrase de passe que votre Tails actuel ainsi la phrase de passe est facile à retenir. Lorsque le paramétrage du stockage persistant affiche la liste des options possibles, cliquez sur Enregistrer et quittez. Le processus de sauvegarde décrit ci-dessous écrase la configuration du stockage persistant. Par conséquent, les options que vous activez ne sont pas importantes lorsque vous créez le stockage persistant. Éteignez et débranchez votre clé USB Tails.

Créer ou mettre à jour votre sauvegarde

1) Démarrer sur votre Tails actuel et déverrouiller le stockage persistant.

2) Branchez votre clé USB Tails de sauvegarde.

3) Aller dans Applications ▸ Outils système ▸ Back Up Persistent Storage. => *À chaque fois que vous mettez à jour votre sauvegarde, seuls les fichiers qui ont changé sont copiés.*

4) Si votre Tails de sauvegarde contient une version qui n'est pas à jour, nous vous recommandons de le mettre à jour en même temps.

Récupérer ses données sur une clé Tails défectueuse

Ca se fait par terminal avec des droits d'administrateurices. Procédure à retrouver sur l'article *Récupérer le stockage persistant d'un Tails endommagé* de la documentation Tails.
https://tails.boum.org/doc/first_steps/persistence/rescue/index.fr.html

pour te protéger). Pour cela au démarrage, dans la fenêtre du Tails Greeter il faut faire le petit + et enlever ***l'usurpation de l'adresse mac.***

Risque : Enlever l'usurpation de l'adresse mac peut avoir des conséquences :

- Qu'on puisse suivre ta position géographique au niveau du réseau.
- Relier ton adresse mac (et donc potentiellement ton identité) à une connexion.
- Identifier ton ordinateur comme étant utilisateur de Tails.
- Dans les lieux avec plusieurs utilisateur.ices d'ordinateur, savoir que c'est ton ordinateur qui s'est connecté à telle heure sur ce réseau.

▪ Impossible d'installer des nouveaux logiciels

Nécessite d'avoir un mot de passe administrateur.

Il est déjà arrivé que le gestionnaire de paquet synaptic refuse d'installer des logiciels. Dans ce cas là, la solution avait été de passer par un `terminal superutilisateur`. (installation par la commande **apt-get update && apt-get install [nom_du_paquet]**)
Si tu vois un message du type : « *[INFO] E: Splitting of clearsigned file /var/lib/apt/lists/vwakviie2ienjx6t.onion_debian_dists_buster_InRelease failed as it doesn't contain all expected parts* », dans ce cas attends plusieurs minutes dans ta cession avant de réessayer. Si ça perdure essaye dans le terminal superutilisateur : **rm /var/lib/apt/lists/*** et refait la première commande.

▪ Rajouter des polices de caractères à Libre office

Pour cela il faut créer dans le « dossier personnel » un dossier « **.fonts** » (ce nom exactement) dans lequel tu peux mettre toutes tes polices de caractères (fonts). Le point avant signifie que ce dossier sera considérer comme un *fichier caché* (Pour le faire apparaître, taper ctrl h). Ce dossier disparaîtra à la fin de la cession, il faudra le remettre à chaque démarrage de Tails. Pour que l'ajout des nouvelles polices de caractère soit pris en compte, il faut éteindre complètement Libre office s'il était ouvert, et le rouvrir.

Pour rendre persistant ce dossier, il faut activer `dotfiles` dans la persistance (vérifier dans `Applications ▸ Tails ▸ Configurer le stockage…`). Tu copies ce dossier .fonts puis tu le colles dans `Emplacements ▸ dotfiles`.

▪ Bridge (ponts), devoir masquer que t'utilises Tor

Si tu ne veux pas qu'au niveau de ton fournisseur d'accès internet on sache que tu utilises Tor (par exemple lorsque tu es dans un pays où Tor est soit interdit soit dangereux ou suspect), il est possible d'utiliser un « ***bridge*** » (en français un pont). Il s'agit d'un nœud ***non-public*** de Tor, donc moins connu. Tails en a par défaut. Il peut être, dans certains contextes, utile d'avoir des ponts personnalisés qui sont donc moins connus.

Tu peux alors trouver des ressources pour avoir accès aux bridge dans la documentation Tails à l'article « Se connecter au réseau Tor » :

https://tails.boum.org/doc/anonymous_internet/tor/index.fr.html

J'ai perdu toutes mes clés pgp dans Thunderbird !

Nécéssite des droits d'administrateur.ices

Dans `Thunderbird ▸ ☰ ▸ Outils ▸ Gestionnaire de clés Openpg` il n' y a subitement plus rien suite à un bug. Il existe une sauvegarde de la version avant perte de te clé qu'on

▪ Darkweb / deepweb, qu'est-ce que le .onion ?.....32
▪ Pour pouvoir utiliser les .onion dans la pratique quotidienne avec ta persistance 32
▪ Paramètres de sécurité du navigateur Tor.....32
▪ Sites qui censurent Tor.....33
> Outils supplémentaires.....34
Vérifier que son matériel informatique n'a pas été modifié.....34
III) Astuces / bugs récurrents sur Tails.....35
▪ L'ordi essaye de démarrer sur la clé mais ça ne marche pas.....35
▪ Ma clé Tails ne veut plus démarrer ! (alors qu'elle démarrait avant sur l'ordi).....35
▪ Je configure un logiciel (comme Thunderbird), mais au redémarrage je perds tout.....35
▪ Y a des choses qui ne marchent pas avec ma clé Tails / signaler un problème.....36
▪ Subitement je n'ai plus accès à ma persistance malgré le fait qu'elle soit activée.....36
▪ Je n'ai plus d'espace libre sur une clé usb ?.....36
▪ Un fichier s'ouvre toujours en lecture seule ou ne s'ouvre pas ?.....37
▪ Impossible d'installer des nouveaux logiciels.....38
▪ Rajouter des polices de caractères à Libre office.....38
▪ Bridge (ponts), devoir masquer que t'utilises Tor.....38
> Pense à faire des sauvegardes !.....39
Pour aller plus loin quelques sites :.....40
Listes de logiciels et de services alternatifs 40
Site d'info et d'analyse 40
Outils pédagogiques.....41
Autres.....41



Quelques explications

The Amnesic & Incognito Live System

Tails est un ***système d'exploitation***. Tout le monde connaît les systèmes d'exploitation. Si je vous dis « Windows » ou « Mac », ça devrait vous parler. Je devrais préciser *Mac Os X* pour être exact, ou *Windows 8* pour préciser la version. Un **système d'exploitation** représente l'ensemble des programmes qui pilote les différents composants (disque dur, écran, processeur, mémoire etc…) de l'appareil informatique et lui permet donc de fonctionner.

D'autres systèmes d'exploitation existent. Peut-être avez-vous déjà entendu parler de *Linux* ou de *Ubuntu* ? Dans la famille Linux, on trouve une sous-famille qui s'appelle *Debian* (prononcez « débiane »). Et dans cette sous-famille, on trouve *Ubuntu* et *Tails*. *Tails* est une distribution (une version) de Linux.

- Tails est un système dit **live**. Ça veut dire qu'il ne s'installe pas sur un ordinateur. Il s'installe généralement sur une clé USB (ou une carte SD ou même un DVD). Lors de son utilisation, l'ordinateur fonctionne uniquement sur cette clé. D'ailleurs, cet ordi peut ne pas avoir de disque dur, son système d'exploitation habituel peut être complètement planté ou surchargé, peu importe, ça marchera pareil, il ne s'en servira pas.
- C'est ce qui lui permet d'être **amnésique.** Par défaut Tails est conçu pour ne pas laisser de traces sur l'ordinateur une fois que la session est terminée. La clé utilise uniquement la mémoire vive de l'ordinateur (mémoire plus volatile que le disque dur), qui est nettoyé à l'extinction. Elle est faite aussi pour, par défaut ne pas installer de nouveaux logiciels (même si on verra que c'est possible) et revenir à son état initial après chaque redémarrage.
- Tails est aussi un système qui vous permet d'être **incognito**. Il cache les éléments qui pourraient révéler votre identité, votre localisation, le contenu de ce que vous échangez, etc.
- Tails est conçu pour faire de la **sécurité informatique,** elle est aussi bien utilisée pour des activistes, journalistes, toutes personnes souhaitant limiter ses traces numériques (pour des raisons politiques ou de protection), des mafieux, des militaires,… Un environnement minimal, fonctionnel et vérifié est déjà installé (avec de quoi faire un minimum de traitement de texte, traitement d'image, de son, de vidéos,…). Elle intègre des outils de chiffrements et de suppression de données qui se veulent simples et tout un tas de protections contre un certains nombre de types d'attaques sont pensées.

La sécurité numérique d'aujourd'hui ne vaudra plus rien demain. **La protection des données personnelles passent par les mises à jour, il est important de les faire dans des délais raisonnables**. Il n'existe pas d'outils informatiques de protection de données fiables s'ils ne sont jamais mis à jour, et pour avoir durablement confiance dans ces outils, il est bien de vérifier que des équipes travaillent en continu dessus, qu'elles sont réactives, et de voir quelle est leur réputation sur le net.

cliques en haut sur la petite flèche ▾, « `afficher les fichiers cachés` ». Là tu vas avoir de nouveaux fichiers en *.quelque_chose*. Le fichier *.Trash-10xx* au sein de ta clé usb, c'est ta corbeille (et si tu mets à la corbeille ta corbeille elle va être complètement enlevée), attention d'autres fichiers cachés peuvent être important à garder dans d'autres espaces notamment dans le dossier personnel de ta clé Tails.

▪ Un fichier s'ouvre toujours en lecture seule ou ne s'ouvre pas ?

… alors qu'il n'y a pas déjà le même fichier d'ouvert et qu'avant ça marchait ? Même astuce que le paragraphe d'au-dessus. Tu fais *Afficher les fichiers cachés.* Un fichier en *.lock* avec avant le même nom que le fichier qui te pose souci. Supprime ce fichier, il indique à la persistance qu'il serait déjà ouvert ailleurs. Si c'est pas ça, il faut changer les droits de permission du document.

▪ Je n'arrive pas à installer Tails sur une clef usb

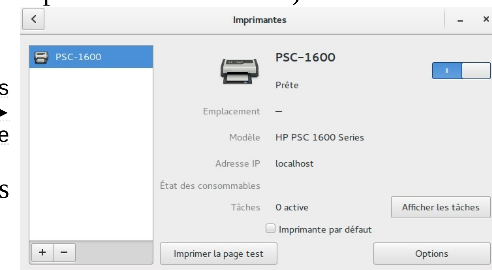
Vérifie que ta clef usb n'est pas connue pour ne pas marché sur Tails : https://tails.boum.org/support/known_issues/index.fr.html. Formate toi même l'intégralité de ta clé usb et essaye de relancer l'installation.

(Pour formater ta clé : `Applications ▸ Utilitaires ▸ Disques`. Là **tu sélectionnes ta clef usb**, ▸ ≡ (en haut à droite de l'écran disques) ▸ Formater le disque.

▪ Un logiciel fait ramer Tails? L'écran frise ?

Essaye d'appuyer sur la touche *windows* , ou la touche Cmd pour Mac (c'est un peu une touche magique quand ça frise) qui ouvrira la fenêtre avec toutes tes applications en cours, applications que tu peux éteindre en faisant la petite croix (si en appuyant sur cette touche ça défrise pas, t'es parti.e pour éteindre de force).

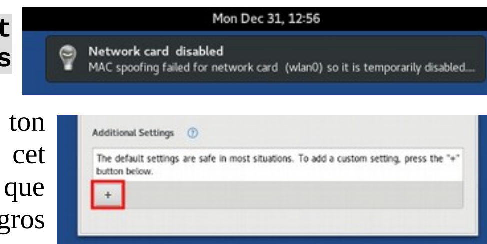
▪ Ajouter une imprimante



Tu vas dans : `Applications ▸ Outils système ▸ Paramètres ▸ Périphériques ▸ Imprimantes ▸ « + » ▸ Ajouter une imprimante.`

Certains modèles d'imprimantes peuvent ne pas fonctionner (ou difficilement) avec Tails.

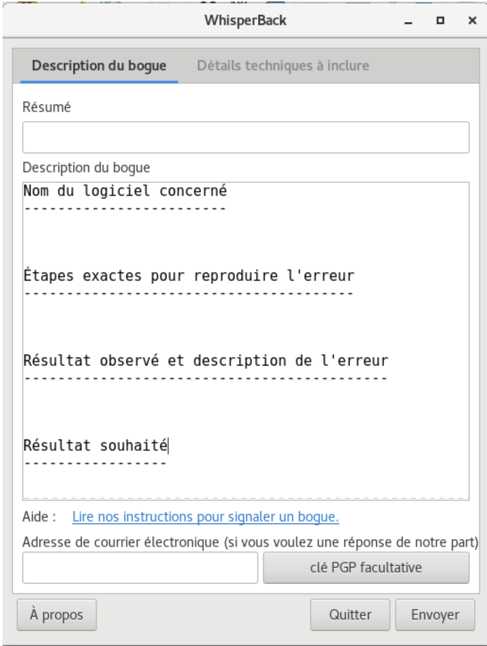
▪ Je n'arrive pas à avoir internet dans certains lieux où j'avais identifié mon ordinateur



… comme la fac, certains lieux publics. Si ton ordinateur était identifié pour ouvrir internet à cet endroit pour pouvoir y utiliser le wifi, il faut que Tails arrête d'usurper l'adresse mac (c'est en gros l'identité de ton ordi, Tails l'usurpe automatiquement

`navigateur non sécurisé` (qui est firefox mais avec très peu de fonctions). Tu tapes un url basique (genre perdu.com) pour accéder à ta page d'authentification. Une fois l'identifiant mis, t'attends que *Tor soit prêt* pour aller sur ton navigateur Tor, puis tu fermes le navigateur non sécurisé le but n'est pas d'utiliser ce navigateur non sécurisé. Un.e attaquant.e malveillant peut essayer d'utiliser le navigateur non sécurisé pour récupérer ton adresse IP, c'est pour cela qu'il vaut mieux le fermer une fois que tu te mets sur le navigateur Tor.

▪ Y a des choses qui ne marchent pas avec ma clé Tails / signaler un problème



Ça peut venir de ton ordi, de ta clé ou de ce que t'as installé. Ça peut venir de ta clé Tails (bug de Thunderbird,...), tu peux essayer de réinstaller Tails dessus.

Ça peut venir des ordis qui ne sont pas tout à fait adaptés à Tails. Par exemple certains modèles d'ordis n'activent pas la wifi avec Tails. Regarde à la page ***problèmes connus*** s'ils n'en font pas état (avec parfois des solutions). s'il n'y a pas, tu peux utiliser l'outil pour signaler une erreur. S'il ne faut pas l'utiliser à la légère pour ne pas surcharger les personnes qui travaillent sur Tails, c'est aussi une manière de contribuer à Tails car iels peuvent à partir de ces données soit proposer une solution s'il y a, soit rajouter à la liste des problèmes connus et essayer de trouver une solution pour les prochaines versions de Tails. Tu vas dans *`Applications ▸ Outils système ▸ Signalement d'erreur`* …

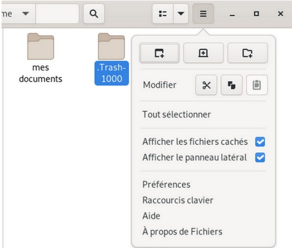
Il est important d'être aussi précis.e que possible dans l'énonciation du problème, et, si c'est possible, pour aller plus vite, de traduire en anglais.

▪ Subitement je n'ai plus accès à ma persistance malgré le fait qu'elle soit activée

Alors sache d'abord que ta persistance est toujours accessible à partir d'un autre système d'exploitation (de préférence une autre clé Tails). Tes données sont là, ça doit être le lien vers ceux-ci qui n'existent plus. Démarre avec la persistance, va voir dans *`Applications ▸ Configurer le stockage persistant`*. Si ça te propose de mettre un mot de passe, mets le même qu'avant et recoche les cases, redémarre ça devrait être bon.

▪ Je n'ai plus d'espace libre sur une clé usb ?

Si tu n'as plus de place sur une clé usb de stockage ou s'il y a plus de données indiquées que réellement présentes sur ta clé tu



Il faut bien comprendre l'état d'esprit de *Tails* : tout y est fait pour être sécurisé au maximum. Cependant en informatique il n'existe pas d'outil tout puissant, il y a toujours des limites (on verra à la fin de la brochure quelques unes). Qui plus est **la manière dont vous utilisez Tails peut générer des failles**.

Des inconvénients existent, qui découlent de la volonté d'être amnésique et incognito : espérance de vie moindre d'une clé usb, possibilité de la perdre ou d'oublier sa phrase de passe (et toutes les données qui vont avec), difficulté d'utiliser certains outils non programmés par défaut, limites de la mémoire vive.

Tails est un « logiciel » libre. **Chacun·e peut en consulter le code source (la recette), le récupérer, le modifier, et le redistribuer tel quel ou modifié** …

Tails essaye de fonctionner au maximum par dons afin d'être indépendant et d'avoir des outils permettant d'améliorer la sécurité. Son coût est estimé à 6 euros par an et par utilisateurices. De la même manière il est possible d'aider de plein de manières possibles son fonctionnement (même sans être geek, par exemple la traduction)[1].

Les outils et services utilisés (Tails, Tor, Riseup,...) sont des services à prix libre, mutualisés, militants, accessibles à tou·tes et qui ne vivent QUE par l'implication de tou·tes (en temps, argent ou autre).[2]

Par contre, il faut absolument s'assurer que la version de *Tails* en ta possession soit saine. C'est essentiel. Ne néglige pas les étapes de vérification. Heureusement, des outils existent pour ça, et sont bien vulgarisés sur le site de Tails.

▪ Notion de modèle de menace

Tails n'est pas magique et comporte plein de limites. Les internets et l'informatique sont des mondes de truands qui ont leur économie et leur pouvoir basé sur le vol de données. Tails ne vous protège pas des failles humaines, de mouchards matériels directement intégrés à l'ordinateur, d'un mouchard logiciel sur le bios, d'être vérolé, ou de certains types d'attaques. Il n'existe pas de sécurité absolument parfaite sur internet, d'où l'intérêt de pouvoir faire un modèle de menace en informatique :

Contre qui je me défends, quels sont ses moyens, quelles sont les conséquences s'ielles ont accès à telles données, quels moyens je peux mettre en œuvre. En fonction de ça des réponses différentes peuvent être posées.

Ce modèle de menace est important à comprendre. Il ne fait aucun sens de dire « tel outil est safe / sécurisé », ça dépend toujours de ce modèle de menace et à quel niveau (réseau, matériel, logiciel, local, etc). Pour plus d'informations détaillées à ce sujet, consulter le **guide d'autodéfense numérique** (https://guide.boum.org/).

1 Pour cela on peut se référer à ce lien : https://Tails.boum.org/contribute/index.fr.html
2 Pour consulter des sites qui proposent des logiciels ou hébergements avec de la sécurité informatique vous pouvez fouiller par ici : https://riseup.net/en/security/resources/radical-servers, ou par ici : https://prism-break.org/fr/

I) Bases pour utiliser Tails

Préalable

Tails ne marche pas avec des ordinateurs en 32 bit (vieux ordis, la plupart sont en 64 bits). Il marche uniquement sur des clés usb de plus de 8 Go sur des DVD, si c'est un DVD il n'est pas possible d'avoir de persistance (ou éventuellement sur une machine virtuelle). Les données seront complètement effacées à l'installation, donc sauvegarde avant tes données ailleurs, et si tu veux qu'on ne retrouve pas de traces de ce qu'il y avait avant consulte la partie « **supprime vraiment tes données** ».

Certains modèles d'ordinateurs ou de clé usb ne fonctionnent pas avec Tails, ou certaines fonctionnalités ne marchent pas, ou parfois il faut des astuces pour la faire marcher. Pour savoir cela n'hésite pas à consulter la documentation de Tails qui recense certaines de ces problématiques[3].

Si c'est trop lent, il est possible d'augmenter la RAM de ton ordinateur (mémoire vive), y en a pas mal sur *leboncoin* par exemple, n'hésite pas à y mettre 4 Go ou plus (ça marchera difficilement avec moins).

Comment utiliser ce tuto ?

Ce tuto est en plusieurs parties : la première comporte plutôt les bases pour se lancer sur Tails, certaines parties abordent plus des cas spécifiques (à voir celui qui peut te concerner). La 2e partie comporte des astuces, sur des logiciels intégrés dans Tails. Dedans il y a aussi des éléments qui sont plus complexes / moins nécessaires pour utiliser Tails. La 3e porte plus sur des astuces et bugs que tu risques de rencontrer avec ta clé Tails (pour éviter de la mettre de côté dès le 1er problème, le plus souvent la solution est simple), ainsi que les marches à suivre pour faire des sauvegardes de ta clé Tails.

Une partie de ce tuto vient de copiés-collés d'autres tutos déjà existants, un peu mis à jour.

3 Que tu peux retrouver sur la page « Problèmes connus » : https://tails.boum.org/support/known_issues/index.fr.html

III) Astuces / bugs récurrents sur Tails

▪ L'ordi essaye de démarrer sur la clé mais ça ne marche pas

Vérifie les messages d'erreurs affichés (si t'as un vieil ordi en architecture 32 bit par exemple ça ne pourra pas marcher sur Tails). S'il y a marqué `Error starting GDM with your graphics card`, ça vient de la carte graphique, consulte la page « Problèmes connus avec des cartes graphiques » du site de Tails.

Si t'as la page d'amorçage de Tails, essaye de démarrer sur le « mode sans échecs » (*Tails troubleshooting mode*). Tu peux aussi consulter la liste des problèmes connus du site de Tails si des solutions ne sont pas proposées en cherchant le modèle de ton ordi.

▪ Ma clé Tails ne veut plus démarrer ! (alors qu'elle démarrait avant sur l'ordi)

Suite à une mise à jour, à une mauvaise manip, ou autre, Tails ne démarre plus sur mon ordi. 3 possibilités sont toujours là :

1) Je vais voir la ***documentation de Tails*** par exemple sur la page qui parle des problèmes de la mise à jour effectuée.

2) Je fais une ***mise à jour manuelle*** (plus haut dans le document), par exemple dans le cas ou la clé a été éteinte avant la fin de la mise à jour.

3) Rien à faire, les 2 premières solutions ne marchent pas (cas par exemple de clé usb trop vieille, de mauvaise qualité ou qui a été malmenée). Essaye de récupérer tes données en branchant cette clé sur une autre clé Tails allumée (elle apparaitra comme une clef usb normale où tu dois taper ton mdp). Si ça marche, crée une nouvelle clé Tails et clone ton ancienne. (chapitre *sauvegarder sa clé Tails*). Si tu peux pas accéder à tes données sur une autre clé Tails alors que t'avais une persistance active, ta clé usb est peut être morte.

Cas particulier : La dernière version de Tails ne marche pas ou a un bug chez moi (à cause de l'ordi ou de la clé). Ça arrive, remets la version Tails d'avant ou va voir la page des nouveautés de Tails[14] souvent iels parlent de la dernière mise à jour, des bugs qui ont été remontés.

▪ Je configure un logiciel (comme Thunderbird), mais au redémarrage je perds tout

Soit t'as oublié d'activer ta persistance avant de faire les configuration, sinon va voir dans `Applications ▸ Tails ▸ Configurer le stockage persistant` et regarde si ton logiciel est coché.

▪ Se connecter à un réseau wifi public (ou un réseau qui nécessite une page d'authentification)



Il faut d'abord demander l'autorisation à Tails d'avoir accès à un navigateur non sécurisé. Au démarrage, dans le Tails greeter (page *Bienvenue dans Tails!*), faire le `« petit plus » ▸ navigateur non sécurisé ▸ oui.` Une fois dans Tails tu te connectes à la wifi publique, puis tu ouvres `Applications ▸ internet ▸`

14 https://Tails.boum.org/home/index.fr.html

libre (cf liens sur la dernière page de cette brochure), certains sites censurent d'un côté Tor mais proposent des services en .onion pour les gens qui sont dans des pays où leur site est censuré (par exemple facebook[11]), si sncf-connect.com bloque la possibilité de voir les horaires des trains par Tor, son concurrent non[12], si youtube te bloque tout le temps tu peux passer par une instance de invidious qui l'utilise à ta place[13]. Sur ce site, il existe le chapitre « *Accès plus sécurisé aux services non fiables* » qui recense d'autres sites alternatifs https://technopolice.be/autodefense-numerique/.

Remarque : Tu peux changer le circuit du navigateur Tor en faisant le petit pinceau (sauf le 1er nœud) qui fermera dans la foulée tous tes onglets ouverts, remettra à zéro le statut de la session incluant le cache, l'historique, et les cookies (sauf les cookies protégés par la fonctionnalité de « Protection de Cookies »). Ça peut parfois **permettre d'aller un peu plus vite dans la navigation** (on peut passer par des nœuds avec une bande passante plus rapide) ou encore limiter les liens entre 2 travaux sur le navigateur. Pour changer les circuits Tor que tu utilises tu peux aussi déconnecter et reconnecter la connexion internet.

Attention : En fonction du modèle de menace, cette fonctionnalité ne suffit pas à correctement séparer des identités contextuelles dans le contexte de Tails, du fait que les connexions en-dehors du Navigateur Tor ne sont pas redémarrées et que tu conserves le même relais initial du réseau Tor. Redémarrer Tails est une meilleure solution.

> Outils supplémentaires

Vérifier que son matériel informatique n'a pas été modifié

Techniques de preuve de falsification pour du stockage en milieu sensible, ou envoies par la poste de clé Tails ou ordinateurs. Lire l'article : « Mosaïque aléatoire - Détecter un accès physique non autorisé avec des haricots, des lentilles et du riz coloré » (article en anglais). https://dys2p.com/en/2021-12-tamper-evident-protection.html

Filtre de confidentialité

Protection à rajouter sur l'écran pour empêcher les personnes ne se trouvant pas en face de l'écran d'y voir le contenu. Lorsque tu travailles dans des espaces avec beaucoup de passages.

11 Tu trouveras facilement l'url en tapant facebook .onion sur internet, cependant si t'as besoin d'avoir un compte facebook réellement anonyme il y a d'autres réflexion à avoir. Quelques ressources dans le texte « face à facebook » sur inkiosques.net : https://infokiosques.net/spip.php?article1725

12 https://www.trainline.fr/

13 Par exemple sur France data network : https://invidious.fdn.fr/, **tu peux retrouver des instances corrects d'invidious** ici : https://github.com/iv-org/documentation/blob/master/docs/instances.md. Il existe aussi piped qui offre des services équivalents : https://piped.kavin.rocks/. Si tu souhaites ne pas avoir de trackers google – notamment si t'utilises le service hors tor - il faut rajouter &local=1 à la fin de ton url, ou créer un compte et le configurer pour cela.

Installation

Pour installer *Tails* sur une clé, il te faut une « source » et …une clé USB d'une capacité supérieure à 8 Go.

Concernant la « source », deux solutions :

▪ [SOLUTION 1] Installation à partir d'une autre clé Tails

Ça consiste à trouver un·e utilisateurice de *Tails* en qui on a confiance. Car dans *Tails*, un petit logiciel très simple permet de créer une nouvelle clé *Tails* en quelques minutes et trois clics. La procédure est expliquée plus loin dans cette brochure. En plus, ça permet d'en discuter avec quelqu'un·e, et de voir des vrai·es gen·tes dans la vraie vie. L'inconvénient de cette méthode c'est que si cette source n'a pas été vigilante elle peut diffuser une clé vérolée (cf partie *clé vérolée*).

> Près de chez toi existe probablement un·e utilisateurice de Tails ! Rapproche-toi des assos qui défendent les logiciels libres, des fournisseurs d'accès à internet (FAI) associatifs, des hébergeurs militants, etc … (tou·tes ne font pas forcément de la sécurité informatique) Tu peux jeter un coup d'œil à l'agenda de l'asso *April*, avec des rendez-vous fréquents dans toute la France, ici :
> https://www.april.org/aggregaTOR/sources/1
>
> Ou une petite liste de FAI associatifs là :
> https://www.ffdn.org/fr/membres

▪ [SOLUTION 2] Installation par téléchargement

Il faut suivre le guide d'installation de *Tails* téléchargeable depuis le site *https://Tails.boum.org/install/index.fr.html*. A partir de là le site de Tails t'accompagnera pas à pas, il est important de suivre la totalité du tutoriel qui est très bien fait.

> Booter sur ta clé Tails

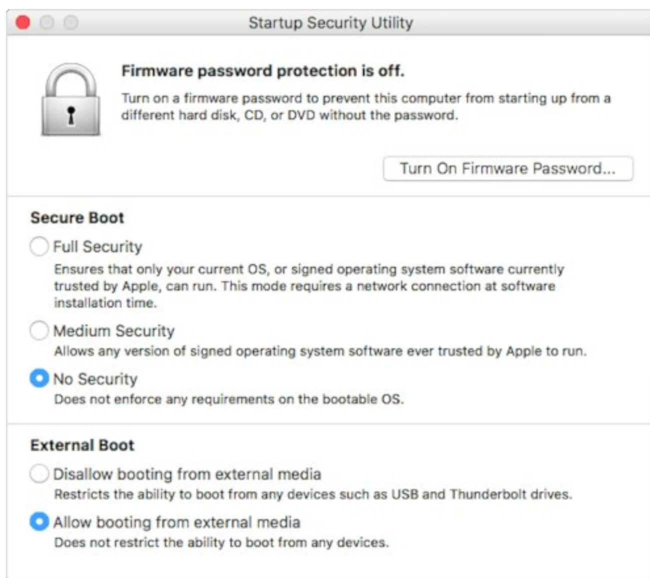
Pour les Mac

La première chose à essayer est, tout de suite au démarrage, d'appuyer de manière continue sur la touche **Alt** (appelée touche options), ou le symbole est quelque chose comme : ⌥ . L'écran qui devrait suivre comportera deux icônes, dont l'une représente une sorte de clé usb et est sous-titrée



« *EFI Boot* » (voir l'image ci-dessous, attention parfois ça a un autre nom, parfois ça s'appelle windows car mac croit qu'il n'existe pas d'autre système d'exploitation que lui même et windows). Clique dessus, et tu devrais obtenir l'écran de démarrage de *Tails*.

Si ton Mac affiche l'erreur suivante : *Vos réglages de sécurité ne permettent pas de démarrer ce Mac depuis un disque de démarrage externe.*



Alors tu dois changer les paramètres de l'*utilitaire Sécurité au démarrage* de ton Mac pour autoriser le démarrage depuis Tails. Pour ouvrir l'*utilitaire Sécurité au démarrage* :Allume ton Mac, et reste appuyer sur **Command(⌘)+R** immédiatement après que tu vois le logo Apple. Tu devrais tomber sur le macOS Recovery[4]. Choisis **Utilities ▸ Startup Security Utility** dans la barre de menu. Lorsque l'on te demande de t'authentifier, clique sur *Enter macOS Password*, puis choisis un compte administrateur et entre son mot de passe.

Dans le Startup Security Utility:

- Choisis **No Security** dans la section **Secure Boot**.
- Choisis **Allow booting from external media** dans la partie **External Boot**.

Pour les PC

Il faut au démarrage configurer le *bios*. Le « bios », parfois c'est marqué *startup enter* ou *enter setup* (ou pour les ordis récents on va chercher « *UEFI* ») est un logiciel qui vient avant que l'ordi démarre sur le système d'exploitation, il gère notamment le démarrage de ta machine, en lui disant quel disque utiliser pour commencer à faire quelque chose.

Au moment ou tu démarres il faut appuyer la plupart du temps sur **F2**, ou **F12,** ou **F6,** ou **suppr,** ou **echap**, ou une touche spéciale, ou parfois une combinaison de touches… Des fois il y a une touche spéciale pour aller sur le bios (si tu vois une touche bleue qui correspond à rien sur d'autres ordi) t'appuies dessus une fois éteint et ça fait démarrer sur le bios.

4 https://support.apple.com/en-us/HT201314

attribuées pour certaines publications. Il est bien plus compliqué de se défendre d'une entité plus puissante qui mesurerait tout ce qui entre et sort du réseau Tor.

Il existe aussi sur internet des scripts avec certaines failles qui peuvent révéler ton adresse IP malgré Tor. Pour limiter cela, ***il est important de tenir Tails à jour,*** il est aussi possible d'augmenter les paramètres de sécurité du navigateur Tor : Tu cliques sur le bouclier 🛡 puis « `Paramètres de sécurité avancée` ». Par défaut il est en *normal*, ce qui correspond à une qualité de navigation qui ne change quasiment pas d'un navigateur normal. Il est possible d'augmenter ce niveau pendant la session, ça enlèvera certains scripts réputés pouvant avoir régulièrement des failles de sécurité. La mise en page de certains sites peut être modifiée, parfois certains contenus ne seront plus téléchargés (images, vidéos,…), ou certains sites ne marcheront pas sans leur donner des autorisations temporaires si on pense pouvoir leur faire confiance.

Niveau de sécurité

Désactive certaines fonctions Web qui peuvent être utilisées pour attaquer votre sécurité et votre anonymat.
En apprendre davantage

◉ **Normal**
Toutes les fonctions du Navigateur Tor et des sites Web sont activées.

○ **Plus sûr**
Désactive les fonctions souvent dangereuses des sites Web, ce qui pourrait entraîner une perte de fonctionnalité de certains sites Web.
JavaScript est désactivé pour les sites non HTTPS.
Certaines polices et certains symboles mathématiques sont désactivés.
Le son et la vidéo (médias HTML5) sont « cliquer pour lire ».

○ **Le plus sûr**
Ne permet que les fonctions de sites Web exigées pour les sites statiques et les services de base. Ces changements affectent les images, les médias et les scripts.
JavaScript est désactivé par défaut pour tous les sites.
Certaines polices, icônes, images et certains symboles mathématiques sont désactivés.
Le son et la vidéo (médias HTML5) sont « cliquer pour lire ».

▪ Sites qui censurent Tor

Il existe plusieurs types de censure du réseau Tor, qui vont de l'image capcha (espèce de jeu pour pouvoir vérifier que tu « n'es pas un robot »), à l'obligation de donner des données personnelles supplémentaires (carte d'identité, numéro de téléphone...) jusqu'à l'impossibilité d'accéder au site.

Cette censure peut cibler **certains nœuds Tor**. Dans ce cas tu peux changer de nœuds de sortie Tor pour ce site (ça ne le fera que sur l'onglet sur lequel tu fais ça – par ailleurs chaque onglet à un nœud de sortie différent). Il faut parfois le faire plusieurs fois si on a la malchance de tomber sur plusieurs nœuds qui se sont vus interdits. Pour ça dans la barre URL, tu cliques sur le cadenas 🔒 . Puis « *nouveau circuit pour ce site* ».

Cette ***censure peut cibler la totalité du réseau Tor***. Ce qui n'est pas si compliqué à cibler pour les sites car tous les nœuds Tor sont publics. Dans ce cas tu peux essayer de *passer par un proxy* pour aller sur le site tel que : https://hide.me/en/proxy (attention uniquement si tu n'as pas à saisir de données personnelles ni à faire des choses sensibles - login, mot de passe, le proxy étant là pour récolter tes données / pouvant compromettre ce que tu fais). Tu peux aussi consulter les archives de la page, avec un peu de chance ta page censuré a été enregistré dessus / accessible par tor : https://archive.org/web/web.php (the wayback machine). Tu peux de préférence passer par des alternatives à ce site : alternative

▪ Darkweb / deepweb, qu’est-ce que le .onion ?

Quelques notions : le « ***deepweb*** » et le « ***darkweb*** » sont des termes inventés par les médias. Le *deepweb*, ce sont des sites qui ne sont pas répertoriés par les moteurs de recherche. Pour y accéder il faut connaître directement l’URL (l’adresse du site), qu’on a pu t’envoyer ou qui a pu être indiqué sur un site internet.

Le *darkweb* concerne les sites qui sont accessibles uniquement par le réseau Tor et ne sont pas non plus répertoriés par un moteur de recherche habituel. Ces sites finissent par ***.onion***. N’importe qui peut mettre un site en .onion. Quand tu sors du 3e relais Tor, tu rentres alors dans le 3e relais Tor du site, puis le 2e puis le 1er. On a donc 6 relais Tor entre nous et le site, nous on connaît les 3 premiers relais, le site les 3 derniers, et chaque nœud Tor connaît juste le relais d’avant et celui d’après. Il s’agit alors, sur le réseau, d’un chiffrement entièrement géré par Tor d’un bout à l’autre.

Contrairement au chiffrement de HTTPS, les adresses de sites en .onion sont longues et compliquées car elles comportent l’empreinte du site. Il n’est plus questions d’autorités de certification (même si quelques sites ont obtenu des certifications reconnus par des navigateurs sur leur .onion), la sécurité passe par le fait de connaître l’empreinte du site.

Certains sites proposent à la fois une URL classique, et une URL en .onion. Dans ce cas, si le site a été configuré pour, une indication « Un .onion est proposé » Un .onion est proposé devrait apparaître, sur lequel tu dois appuyer. Sinon parfois le site l’indique quelque part sur sa page. Pour connaître les sites qui sont uniquement en .onion, il faut soit les avoir par bouche-à-oreille, soit par des sites internet qui recensent d’autres sites en .onion. Il est important de bien vérifier qui propose quoi, car n’importe qui peut proposer n’importe quoi. Attention donc aux arnaqueureuses qui vous proposent des choses. Les sites en .onion ont tendance à avoir moins de suivi dans le temps et il faut suivre l’évolution de l’adresse URL qui peut vite changer…

Quelques exemples de sites en .onion :
Il est possible d’envoyer un document dans un lien en .onion grace à OnionShare présent dans Applications ▸ Internet ▸ OnionShare (ce lien est valable tant que Onionshare tourne et s’arrêtera si t’éteins ta clé).
- *La plupart des sites du réseau mutu en ont un.*
- *Sur ce site des exemples de site en .onion :* *https://github.com/alecmuffett/real-world-onion-sites*

▪ Pour pouvoir utiliser les *.onion* dans la pratique quotidienne avec ta persistance

Tu peux utiliser les *marque-pages* pour ça. Vérifier qu’ils sont activés dans ta persistance dans *Applications ▸ Tails ▸ configurer le stockage persistant*. Lorsque t’es sur ton site en .onion, t’appuies sur l’étoile à droite de l’URL (« Marquer cette page »), tu mets le nom que tu veux à ce marque-page. La prochaine fois t’auras juste à écrire le début du nom du marque-page pour te voir proposer le site en .onion.

▪ Paramètres de sécurité du navigateur Tor

Tor a de multiples limites. Par exemple une entité avec un peu de moyens techniques / juridiques peut, si elle présume que tu te connectes de telle box pour publier sur tel site, essayer de faire des correspondances entre ce qui sort de ta box et entre sur le site. Si le besoin s’en ressent, il peut être intéressant de ne pas passer par des box qui nous sont

Des fois il y a aussi un autre menu qui s’appelle le « *boot order* » ou «option de boot » c’est encore plus simple : tu fais **entrer** sur ta clé ou tu montes ta clé en premier et lances le démarrage.

Fabricant	Touche
Acer	Échap, F12, F9
Apple	Option
Asus	Échap, F8
Clevo	F7
Dell	F12
Fujitsu	F12, Échap
HP	F9, Échap
Huawei	F12
Intel	F10
Lenovo	F12, Novo, F8, F10
MSI	F11
Samsung	Échap, F12, F2
Sony	F11, Échap, F10
Toshiba	F12
autres…	F12, Échap

Bref les solutions sont multiples :

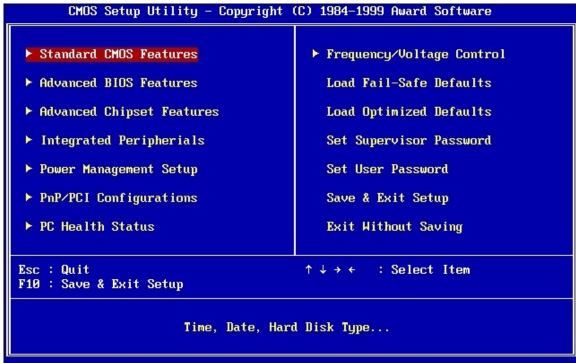
1) Quand t’appuies sur démarrer tu fais des allers-retours en appuyant sur toutes les touches **F,** ainsi que **echap** et **suppr.** La plupart du temps ça marche mais faut bien aller vite. L’inconvénient c’est que des fois y a un autre truc inutile qui démarre sur un autre **Fx** du coup faut redémarrer et faire la même procédure sans ce **F**. Bon des fois ça lance un truc dans le bios en même temps, tu fais *annuler.*

2) Tu sais qu’il faut appuyer sur telle touche, parce que c’est marqué pendant 1 seconde au démarrage, ou parce que tu as tapé le modèle de ton ordi sur internet suivi de bios. Comme on ne sait pas toujours à quel moment exactement il faut appuyer sur la touche en démarrant, à partir du moment ou tu démarres tu appuies plein de fois sur la touche spéciale jusqu’à arriver au bios.

3) Ça peut parfois être plus compliqué si t’as un *windows 10 ou 8* (cf plus loin).
→ *Des fois il faut appuyer simultanément sur la touche **Fn** en même temps que la touche **Fx** pour pouvoir utiliser sa fonction*

▪ Réglage du bios / programme UEFI

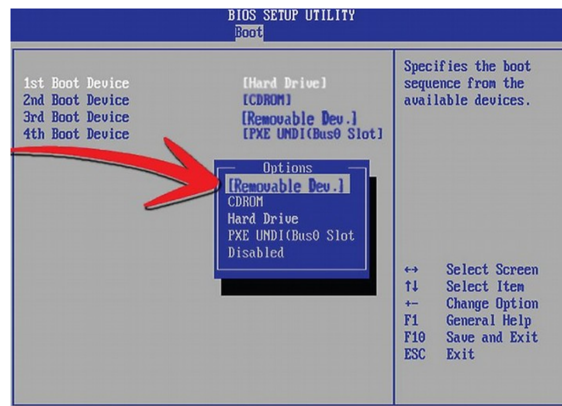




Le bios ressemble souvent à un écran bleu et gris, le plus souvent comme dans la 1re capture écran, plus rarement comme la 3e. Pour naviguer dans le bios c’est marqué quelque part tout ce que tu peux faire. Souvent tu peux juste naviguer avec les flèches, faire **F5** / **F6** ou +/- (parfois d’autres touches) pour « monter / descendre » les options, ou faire **Entrée** pour aller dans un sous-menu ou sélectionner quelque chose.

Une fois dans le bios il s’agit de chercher quelque chose qui s’appelle « boot », « boot order », « boot option » (ou si le bios est en

français c'est donc « ordre de démarrage »). Faut soit chercher le nom de ta clé usb, soit chercher *usb device* ou quelque chose comme ça.



Comment ça fonctionne **:**

L'ordinateur essaye de démarrer sur la 1re option, s'il y a, il démarre dessus, sinon il tente l'option d'en dessous. Ce qui veut dire que :

- si y a le nom de ta clé usb, une fois que tu la retires il rechangera l'ordre de démarrage pour aller sur ton ordi et il faudra aller à nouveau sur le bios pour remettre dans l'ordre.
- Si y a « usb device » il va vouloir démarrer sur une clé usb quand y en aura une, sinon il ira sur ton ordi. Si ton ordi ne démarre pas, c'est peut être qu'une clé usb sans système d'exploitation est branchée et qu'il essaye désespérément de démarrer dessus (dans ce cas redémarre en débranchant la clé usb ou change la configuration du bios)

→ *Des fois y a des options de boot dans le « exit » ou tu peux sélectionner ta clé directement et faire entrer*.

<u>Si tu ne trouves pas ta clé :</u> C'est possible qu'elle soit cachée dans une autre option. Petite astuce : quand y a une petite flèche (⇒) devant une option, tu peux faire **Entrée** et y a des sous-options. Par exemple des fois il faut mettre ta clé en première option dans « hard drive » avant qu'elle apparaisse dans la page d'ordre de démarrage.

<u>En cas de bug</u> <u>:</u> Si ça ne démarre plus sur ton ordi (ce qui est rare), tu peux retourner dans ton bios pour voir l'ordre de démarrage ce qui se passe, si vraiment tu piges pas y a toujours une touche pour remettre ton bios dans les options initiales.

▪ Cas des *windows 8 ou 10* (si c'est la première fois que tu démarres sur un autre système d'exploitation)



Ces petits systèmes d'exploitation ont tendance à mettre plusieurs pièges qu'il va falloir désactiver. Ils peuvent empêcher ou rendre difficile de démarrer directement sur le bios au premier démarrage. Dans ce cas dans windows tu peux essayer de cliquer sur le menu Démarrer puis sur le bouton **Marche/Arrêt** puis, **tout en restant appuyé sur la touche Shift (⇑)**, clique sur **Redémarrer**.

page exacte sur lequel t'es sur le site ou ce qui permet à des intermédiaires de modifier partiellement la page que tu reçois.

Cette sécurisation est essentielle à la fois pour limiter notre empreinte, mais aussi pour ***éviter qu'un intermédiaire modifie le contenu*** de ce que nous envoie un site (puisque l'intermédiaire n'a pas accès au contenu des données, il ne peut pas les modifier partiellement).

Ça c'est la théorie, en pratique plusieurs éléments peuvent compromettre des données sur ce que l'on fait sur le site internet (tracker, éléments d'autres sites sur la page qui peuvent ne pas être sécurisés,...). De plus cette sécurité peut comporter plusieurs limites : la question de comment le site gère ce chiffrement, certains chiffrements ne sont pas assez robustes, comment il gère ses clés de déchiffrement, si on peut lui faire confiance ou non, le fait que beaucoup de sites rajoutes des mouchards (google, facebook, autres sites de pub…). Ça c'est côté confiance liée au serveur du site. Il y a aussi la confiance liée au transport des données.

- Un site peut être ***auto-certifié***, ou avoir une certification non reconnue par le navigateur, dans ce cas un message te demandera de rajouter une exception, de reconnaître cet inconnu qui dit être lui-même. Si tu ne connais pas ses certificats, rien ne t'assure être sur le bon site.
- La plupart du temps le site est ***certifié par une autorité reconnue par le navigateur*** (139 autorités reconnues par Firefox en 2021[9]). Les *autorités de certification* sont des tiers qui ont la capacité de nous certifier que le site sur lequel on va est bien le bon site, d'*authentifier l'identité de ce site / correspondant*. Cette autorité peut être : des entreprises, des organisations, des gouvernements, des banques,… Elle peut délivrer des faux certificats (ce qui veut dire qu'on pense être sur tel site, mais qu'on est en fait ailleurs). Elle peut être usurpée. Et enfin il y a beaucoup d'autorités reconnues par un navigateur, une autre autorité que celle d'origine du site pourrait certifier un faux site, le cadenas vert apparaîtra tout de même.

C'est la limite des autorités de certification, qui peut entraîner l'écoute / la modification du trafic internet (qui s'appelle dans le monde de l'informatique « *attaque de l'homme du milieu* »).

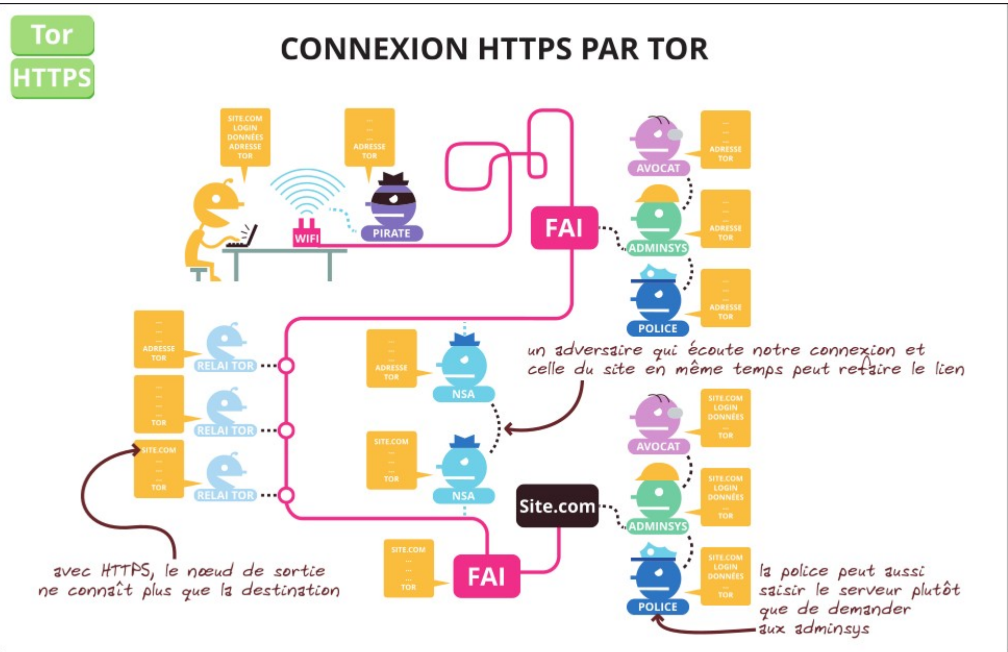
Tor présente l'avantage de ***te protéger jusqu'au 3e relais*** de *l'attaque de l'homme du milieu*, rendant plus compliqué une attaque ciblée, mais cette attaque est possible à partir du 3e relais. On pourrait imaginer une attaque ciblant ce qui sort du réseau Tor.

Je ne développerai pas plus sur ce sujet, on a juste introduit que HTTPS ne te protège pas de tout, n'est pas un chiffrement parfait et ne doit pas t'empêcher de faire attention à ce que tu fais sur internet / à réfléchir à d'autres types de protection. Par exemple utiliser PGP pour chiffrer tes mails, le HTTPS de riseup ne protégera pas le contenu de tes mails de tout, comme dit sur leur site[10]. Pour un chiffrement de bout en bout, il est important que la clé privée de PGP soit stockée en local, et pas sur un serveur distant (comme peut le proposer *protonmail*, attention à leur propagande qui est partiellement mensongère).

9 Liste des autorités ici: https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReport
10 https://riseup.net/en/security/network-security/secure-connections

chiffrées sur le relais 2, elles même chiffrées sur le relais 1. Chaque relais sait seulement d'où ça vient avant, et où elles vont juste après (le relais 3 sait que ça vient de relais 2 et que ça va sur tel site internet après, mais ne connaît pas le relais 1). D'où l'image de l'oignon, le relais déchiffre une première fois mais n'a toujours qu'accès qu'à des données chiffrées, relais 2 pareil, et le relais 3 déchiffre la dernière partie.

Ce qui signifie dans la théorie que tous les intermédiaires jusqu'au relais 1 savent que tu vas sur Tor mais ne sait pas sur quel site tu vas, tous les intermédiaires après le relais 3, savent que quelqu'un·e dans le monde va sur tel site, le site te voit arriver de l'adresse IP du relais Tor.

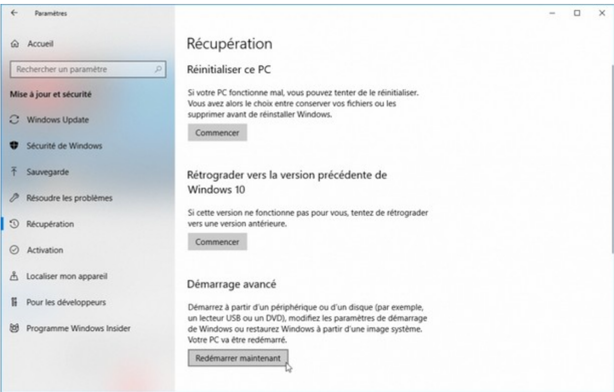


▪ **Qu'est-ce que HTTPS ?**

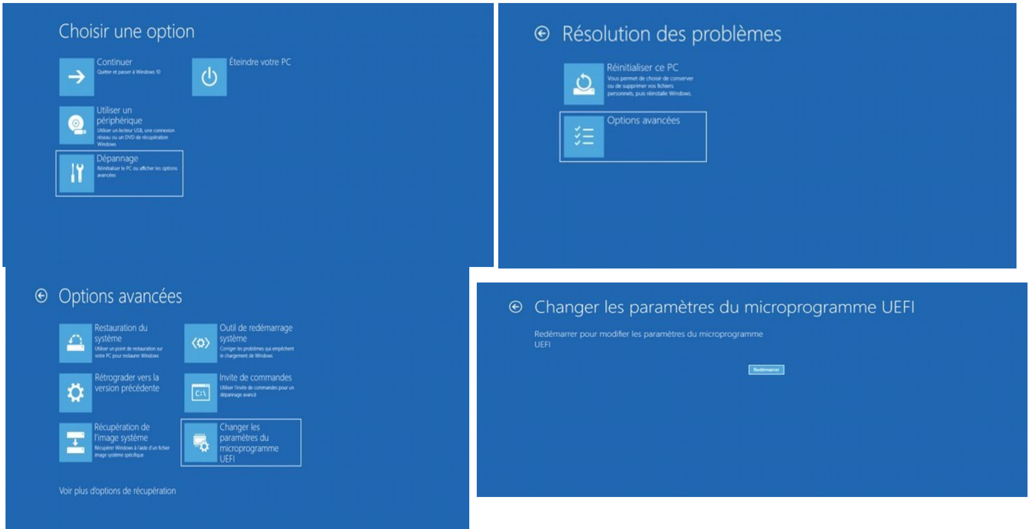
Quand dans l'URL (l'adresse du site) tu vois HTTP:// (s'il n'y a pas de cadenas ou s'il est barré en rouge ou s'il y a un message d'avertissement avant de continuer sur le site en http), cela signifie que la totalité des intermédiaires après le relais 3 du réseau Tor savent ce que tu demandes exactement au site internet (dont tes login, tes mots de passe si on t'en demande). La plupart des sites ont une version « HTTPS », le S est pour « **sécurisé** ». Cela signifie que ce qu'on fait sur le site sur lequel on va est chiffré par une clé de chiffrement qui appartient au site. A partir du relais 3, les intermédiaires sur la ligne sauront qu'on va sur riseup.net par exemple, mais n'auront pas accès à nos mails et à nos mots de passe ni ne sauront si on consulte nos mails ou si on lit une page aléatoirement sur le site. C'est le petit *cadenas* dans l'URL qui apparaît quand t'es en https.

S'il y a un warning jaune dessus, c'est que, dans la page du site, il y a une partie qui n'est pas chiffré (des bouts de http), ce qui peut donner beaucoup d'indication, comme la

Ou alors tu vas, via le menu `Démarrer`, dans `▸ Paramètres ▸ Mises à jour et sécurité ▸ Récupération` en cliquant sur le bouton `Redémarrer maintenant` dans la section `Démarrage avancé`.



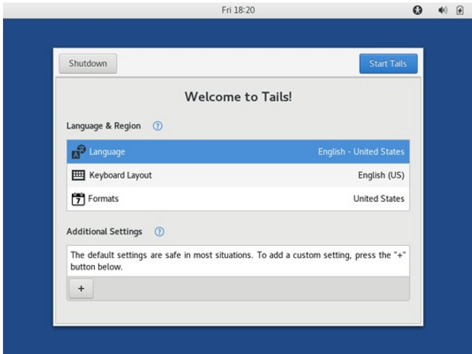
Le menu **Démarrage avancé** de Windows 10 va alors s'afficher.
Clique sur le bouton `Dépannage ▸ option avancée ▸ Changer les paramètres du microprogramme UEFI. ▸ Redémarrer` et tu devrais arriver sur le bios.



Pour la première fois c'est possible qu'il y ait certains paramètres qui t'empêchent de démarrer sur Tails.

- Il est utile de désactiver « fast boot » (dans boot), qui peut au démarrage passer l'étape permettant d'aller sur le bios.

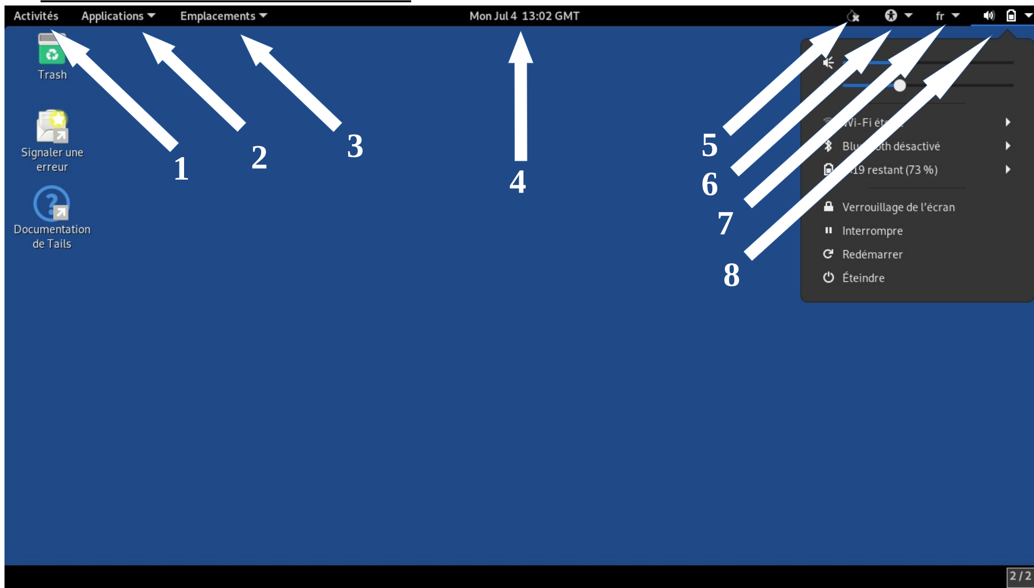
> Démarrer sur Tails



Si l'ordinateur démarre sur Tails, le menu du chargeur d'amorçage apparaît et Tails démarre automatiquement après 4 secondes.
Après 30–60 secondes, un autre écran appelé *Tails Greeter* (Welcome to Tails!) apparaît (qui peut être gris si t'es en mode UEFI).
Dans le Tails Greeter, sélectionne ta langue et ta disposition de clavier dans la section **Langue et région (Pour les utilisateurs d'ordinateur**

Mac, il y a une disposition de clavier pour macintosh). Clique sur **Démarrer Tails.** Quand tu auras activé la persistance, le mot de passe pour l'activer apparaîtra sur cette fenêtre. En attendant tu ne pourras pas stocker de données sur ta clé Tails. Après 15–30 secondes, le bureau de Tails apparaît.

> Utiliser le bureau de Tails



Tails est un système d'exploitation assez classique et simple d'utilisation. Dans la barre supérieure tu trouveras, de gauche à droite :

[1] « Activités » permet de voir les fenêtres et applications dans la vue d'ensemble. Ca permet également d'y faire une recherche parmi les applications, fichiers et dossiers. On peut aussi accéder à « Activités » en envoyant la souris dans le coin en haut à gauche de votre écran ou en appuyant sur la touche Super (⊞) du clavier.

[2] Liste des applications (des logiciels) disponibles classée par thème

[3] Accès aux principaux dossiers (où **apparaît le dossier persistent** lorsqu'il est connecté)

[4] Date et heure. Attention si t'es pas connecté.e à internet, Tails est à l'heure de l'ordi, une fois connecté.e, toutes les clés Tails à travers le monde ont la même heure (il y a un décalage horaire)

[5] Le témoin de l'état de Tor si tu es connecté.e au réseau Tor. Cet outil s'appelle « Oignon Circuits »

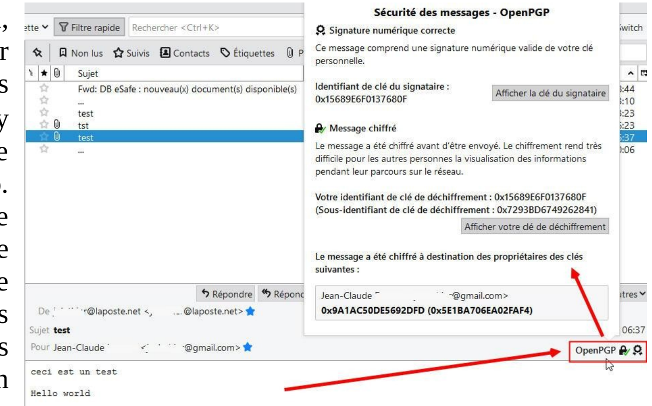
[6] Bouton « Accès universel ». Le menu d'accès universel permet d'activer le lecteur d'écran, le clavier visuel, l'affichage de grand texte et d'autres logiciels d'accessibilité.

[7] choix des langues du clavier.

[8] Le menu système, où tu peux accéder à la luminosité de l'écran et le volume du son, la connexion wifi et Ethernet s'il est branché, l'état de la batterie, le bouton pour verrouiller l'écran avec un mot de passe créé sur le moment (pour quand tu pars et que tu ne veux pas que d'autres gens accèdent directement à ce que tu fais) les boutons de démarrage et d'extinction.

faut avoir que des ok pour envoyer un mail chiffré que tout le monde peut recevoir, ici aussi tu peux changer le statut de tes clés).

Pour chiffrer (ou envoyer un mail non chiffré si t'as cliqué sur « chiffrer par défaut »), il faut cliquer sur la petite flèche à droite de sécurité 🔒Sécurité ⌄ et « exiger le chiffrement » (ou « ne pas chiffrer » si tu n'as pas la clé publique des personnes).



Lorsque tu reçois un mail, s'il est chiffré, tu devrais voir apparaître un petit cadenas coché en vert OpenPGP, s'il n'y a pas ce cadenas, c'est que le mail n'a pas été chiffré par pgp. Le deuxième signe avec le « attention orange » signifie que le mail est signé mais par une clé publique dont tu n'as pas vérifié l'empreinte, si t'as vérifié l'empreinte, l'option apparaît en vert.

▪ Mettre les serveurs .onion de riseup dans Thunderbird

Bonus sécurité - Sensible

Dans Thunderbird, `trois petits traits` ☰ ▸ `préférences` ▸ `paramètres de compte`. Aller dans le paramètre serveur de chaque boite mail à modifier, remplacer **pop.riseup.net** ou **imap.riseup.net** par 5gdvpfoh6kb2iqbizb37lzk2ddzrwa47m6rpdueg2m656fovmbhoptqd.onion (actuellement)

Aller dans *serveur sortant* (smtp), tout en bas à gauche, cliquer 2 fois sur l'adresse mail, remplacer le nom du serveur (mail.riseup.net) par 5gdvpfoh6kb2iqbizb37lzk2ddzrwa47m6rpdueg2m656fovmbhoptqd.onion

Pour vérifier l'adresse du serveur (il n'y a aucune raison de faire confiance à cette brochure), il faut aller sur le site de riseup, à la page `sécurité` ▸ `sécurité réseau` ▸ `Tor` : https://riseup.net/fr/security/network-security/TOR

Pour le premier mail, et à chaque mise à jour des serveurs .onion de riseup, il faudra ***ajouter une exception de sécurité*** pour des questions de certificat la première fois que tu vas aller relever tes mails, et la première fois que tu vas envoyer un mail (après c'est bon). Il peut être important de faire « ***view*** » avant de confirmer le certificat de sécurité, et de vérifier le SHA-256 fingerprint. (procédure complète ici : https://riseup.net/fr/security/network-security/certificates). Pour la réception des mails, un bug dans thunderbird rend impossible d'enregistrer l'exception de sécurité, dans ce cas, dans paramètre serveur, tu peux mettre `sécurité de la connection` ▸ `aucune` (au lieu de Starttls). Attention il ne faut SURTOUT PAS faire ça si tu n'as pas de .onion dans le nom du serveur, sinon t'es informations vont transiter en claire !

> Tor

▪ Qu'est-ce que Tor?

Tor est un logiciel libre associé à un réseau public de plusieurs milliers de serveurs (aussi appelés nœud ou relais). Tor vient à l'origine de **The Onion Router**, il va choisir en avance 3 relais sur le réseau de manière pseudo-aléatoire. Les données recherchées sur internet vont être chiffrées sur le relais 3, ces données chiffrées vont être elles même

correspondant·e puisse vérifier que la clé publique que t'as envoyée t'appartient réellement. Pour que les clés publiques que tu possèdes puissent être utilisable il faut « accepter » ces clés. Un des 2 oui suffit, tu peux cocher le 2ème oui si t'as vérifié avec la personne l'empreinte de sa clé par un autre canal, ça permet de graduer le degré de confiance que t'as envers cette clé et d'être sûr.e de ce qu'on utilise.

Tu ne dois jamais partager ta clé privée, car quiconque en a une copie peut déchiffrer les messages qui te sont envoyés et signer les messages pour qu'ils apparaissent comme provenant de toi.

Si tu n'utilises plus ta clé privée ou qu'elle est compromise il faut révoquer ta clé. Pour cela clique droit sur ta **clé privée** et sélectionne **Révoquer la clé**.

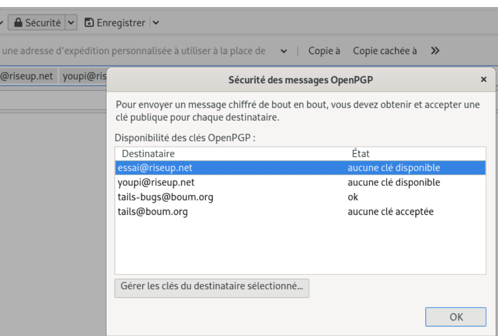
▪ Envoyer sa clé publique / une clé publique d'autres personnes

Quant t'écris un mail dans thunderbird, si t'as activé les options comme dit au dessus, tu cliques sur la flèche à côté de sécurité Sécurité ▸ `OpenPGP ▸ Joindre ma clé publique.` Lorsque le mail sera envoyé, il sera mis en pièce jointe ta clé publique en fichier (un format « .asc »).

Si tu fais un mail à plusieurs personnes, tu dois avoir la clé publique de toutes les personnes à qui t'écris. Si tu veux que les correspondant.es puissent faire répondre à tous de manière chiffrée, il faut qu'iels aient accès aux clés publiques de tout le monde aussi. Pour joindre des clés publiques d'autres personnes, dans thunderbird tu vas dans ☰ ▸ `outils ▸ Gestionnaire de clef Openpgp.` Là tu sélectionnes les clés publiques des différentes adresses mails (ainsi que la tienne), maintenir la touche ctrl enfoncée permet de garder une clé pour en sélectionner d'autres. Puis `clique droit ▸ envoyer une ou des clés par courriel.`

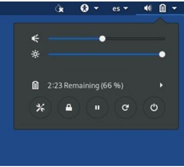
▪ Récupérer une clé publique / envoyer un message chiffré

Tu as une clé privée, ça signifie que les personnes à qui t'enverras ta clé publique pourront t'envoyer des mails chiffrés. Si tu veux chiffrer à ces personnes, il te faut en **première étape** télécharger leur clé publique dans thunderbird. Si une personne t'envoie dans un mail une clé publique (il s'agira sûrement d'une pièce jointe, un fichier dont le nom ressemble à (OpenPGP_)0x[plein_de_chiffres_et_lettres].asc). Tu fais clique droit dessus, *importer une clé OpenPGP* (ou parfois il faut faire *« déchiffrer et ouvrir »)* dans la fenêtre qui suis tu cliques sur « acceptée » ○ Non acceptée (aucune décision) ◉ Acceptée (non vérifiée). Si l'option reste « Non acceptée », la clé publique sera téléchargée dans le trousseau de clé publique mais inutilisable pour chiffrer (pour changer l'option, voir le chapitre « Afficher et gérer les paramètres des clés »). Maintenant tu peux chiffrer tes mails avec cette personne.



Quand t'écris un mail sur thunderbird, tu peux vérifier si tu possèdes les clés publiques des destinatairices en cliquant sur sécurité (il

▪ Pas d'onglet wifi ?



→ si l'onglet wifi n'apparaît pas ici : Regarde si des solutions existent ou si le même problème a été recensé sur ton modèle de carte wifi sur la page « Problèmes connus => le wifi ne marche pas » de Tails[5]. Il se peut que ta carte wifi difficilement utilisables sur Tails. Dans ce cas soit t'as internet par câble Ethernet soit tu te procures une clé wifi (compatible avec Tails comme Panda Wireless Ultra ou PAU05 autour de 15 euros), soit - si tu sais faire - tu changes ta carte wifi.

Tu peux aussi te connecter via les données mobiles d'Iphones/Ipads (pour lesquels le partage Wi-fi ne fonctionne pas. Cependant, « Tails ne peut pas cacher les informations qui identifient ton téléphone sur le réseau local. Si tu connectes ton téléphone à :

- Un réseau Wi-Fi, alors le réseau connaîtra l'adresse MAC de ton téléphone. Cela a des implications en matière de sécurité qui sont discutées dans la documentation Tails sur l'anonymisation d'adresse MAC. Certains téléphones ont une fonction pour cacher l'adresse MAC réelle du téléphone.
- Un réseau de données mobiles, alors le réseau sera capable de connaître l'identifiant de ta carte SIM (IMSI) ainsi que le numéro de série (IMEI) de ton téléphone. »

> Configurer la persistance / stockage de données sur la clé Tails

Tails est ***amnésique par défaut.*** Il oublie tout ce que tu as fait entre deux sessions. Quand on veut travailler sur un document c'est un peu balot. Quand on veut paramétrer Tails c'est tout aussi chiant : on est obligé·e de le refaire après chaque démarrage. Heureusement, les créateurices de Tails y ont ajouté la ***persistance*** !

Le principe est de créer un « endroit » (appelé *volume*) sur ta clé, qui sera entièrement chiffré, sur lequel tu pourras stocker tes documents, et qui sera aussi utilisé par certains logiciels pour y stocker les données que tu auras autorisées. C'est techniquement très simple à faire.

Tu démarres ta clé Tails, tu vas dans `Applications ▸ Tails ▸ configurer le stockage…` *(persistant).* Là une fenêtre s'ouvre ou tu dois taper une phrase de passe et ensuite configurer ce que tu dois conserver dans la persistance. Ensuite, le stockage persistant peut être activé pour plusieurs types de données, en voici quelques détails / explications :

Données personnelles	Stocker des fichiers persos, que tu retrouveras dans le dossier **home>persistent** (via Emplacements => persistent)
Écran de bienvenue	Permet de garder en persistance un mot de passe administrateur, la langue et les paramètres supplémentaires (comme le navigateur non-sécurisé).
Ponts Tor	Lorsque l'option Pont Tor est activée, le dernier pont Tor que vous avez utilisé pour vous connecter avec succès à Tor est sauvegardé dans le stockage persistant.
Marque-pages du navigateur	Tout est dans le titre, pour ton navigateur Tor.
Connexions réseau	Pour se souvenir notamment des mots de passe wifi ou autres configurations de connexionvér

5 https://tails.boum.org/support/known_issues/index.fr.html#no-wifi

Logiciels additionnels	Pour pouvoir ajouter des logiciels à Tails (s'installeront automatiquement à chaque démarrage avec persistance)
Imprimantes	Il s'agit de sauvegarder les configurations des imprimantes.
Thunderbird	C'est un client mail. Ça permet de garder tes configurations et tes mails en mémoire
GnuPG	Sers à chiffrer / signer en dehors de Thunderbird, notamment avec le logiciel Kleopatra.
Client Bitcoin	La configuration et le porte-monnaie Bitcoin sont sauvegardés. (Bitcoin est une monnaie cryptée décentralisée)
Pidgin	Pidgin sert à faire de la messagerie instantanée chiffrée. Activer cette option te permettra de garder les config des comptes, tes contacts, tes conversations …
Client SSH	SSH permet de se connecter à des serveurs à distance. Cette option permet de sauvegarder des config de connexion.
Dotfiles	Utile pour des configurations avancées, afin de dédoubler des fichiers de config dans le répertoire personnel.

Si t'as un doute sur l'activation d'une des options, n'hésite pas à l'activer (sauf écran de bienvenue qui peut générer des difficultés). Tes choix peuvent de toute façon être modifiés en revenant dans ce programme de « *configuration de volume persistant* ».

Pour prendre en compte les changements de configuration ou la création du volume persistant, il faut redémarrer *Tails*. Après le redémarrage, **le premier écran te propose maintenant de mettre un mot de passe de persistance**. Si tu ne le mets pas, la persistance ne sera pas activée mais tu peux tout de même démarrer Tails.

▪ Changer sa phrase de passe

Tu démarres Tails sans la persistance avec des droits d'administrateur (cf partie *définir un mot de passe d'administration*), tu vas dans `Applications ▸ Utilitaires ▸ Disques`. Tu sélectionnes ta clé Tails. Tu vas voir sur cette écran les partitions de ta clé Tails. Tu sélectionne la partition *Tailsdata* avec un petit cadenas fermé, tu cliques sur les roues dentées ▸ `Modifier la phrase de passe`, on va d'abord demander ton mot de passe administrateur, puis tu tapes ton ancienne et ta nouvelle phrase de passe.

▪ J'ai oublié ma phrase de passe

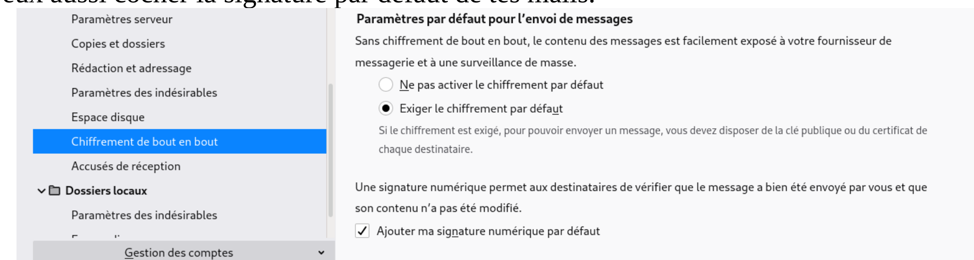
Tu perdras toutes tes données, mais tu peux démarrer Tails sans persistance, puis `Applications ▸ Tails ▸` **`Supprimer le volume d`**… Et `Applications ▸ Tails ▸ Configurer le stockage`… (cf chapitre au début du chapitre).

Quota	**Illimité**. Tu n'auras jamais à t'inquiéter du quota si ton client est configuré pour supprimer les messages sur le serveur après téléchargement.	**Limité**. tu auras un quota limité.
Sécurité	**Haute**. Les messages ne sont pas stockés en permanence sur le serveur (*Note : c'est vrai que si tu fais confiance au serveur mail sur le fait qu'il ne fait pas de copie des mails*).	**Plus basse**. tu dois te fier à Riseup pour le stockage.

▪ Configuration de la clé privée OpenPGP dans thunderbird.

Dans thunderbird, clique sur `Trois petit trais ☰ ▸ Paramètres des comptes ▸ Chiffrement de bout en bout (de la boite mail que tu veux configurer) ▸ Ajouter une clé ▸ Créer une clef openpgp ▸ Continuer ▸ quand tu descends tu mets dans Paramètres avancés, Type de clé « ECC (courbe élliptique) », par défaut c'est RSA, changer permet une sécurité de chiffrement supérieure ▸ Générer la clé ▸ Confirmer.`

C'est bon, ta clé privée est créée. Vérifie que ta clé est bien cochée dans « Chiffrement de bout en bout » du paramètre de compte. Tu peux programmer soit de tout chiffrer par défaut (et quand t'écriras à des personnes qui n'utilisent pas pgp il faudra manuellement décocher l'option de chiffrer), soit de ne rien chiffrer par défaut, ce qui peut comporter un risque d'oublie. Si le chiffrement est important pour toi, il vaut mieux cocher les options « `exiger le chiffrement par défaut` », comme dans la prochaine image. Tu peux aussi cocher la signature par défaut de tes mails.

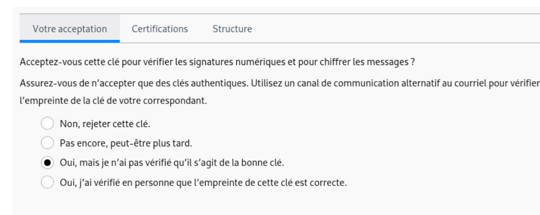


▪ Afficher et gérer les paramètres des clés / vérification de l'empreinte numérique

Une fois que tu as généré ta paire de clés OpenPGP et configuré ton compte de messagerie, tu pourras voir et gérer les paramètres de ton trousseau de clés (les clés privées apparaissent en gras et les clés publiques) en suivant les étapes ci-dessous.

Dans Thunderbird tu vas dans ☰ ▸ `outils ▸ Gestionnaire de clef Openpgp`. Si tu double-cliques sur la clé qui t'intéresse tu pourras accéder à ces paramètres.

Ces fenêtres affichent, entre autres choses, l'ID(entité) des clés publiques que tu possèdes et leur empreinte. Par exemple, l'*ID* d'une clé publique peut ressemble à **0x3EFCD6** tandis que l'**empreinte** complète est **C1CA F701 479E 6C41 D968 0C4B D628 2447 3EFC EFD6**. Cette fenêtre affiche également la date d'expiration de ta clé.



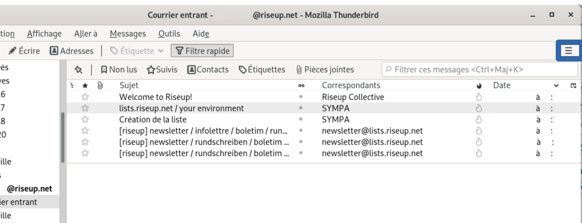
Tu dois partager ta clé publique avec les autres pour qu'iels puissent t'envoyer des messages chiffrés. Tu dois aussi partager ton empreinte complète, via un canal différent, pour que ton/ta

Avec OpenPGP tu peux aussi d'attacher des **signatures numériques** à tes messages. Si tu *signes* un message en utilisant ta *clé privée*, chaque destinatairice ayant une copie de ta *clé publique* peut vérifier s'il a bien été envoyé par toi-même et que le contenu n'a pas été falsifié. De la même façon, si tu as la *clé publique* d'un.e correspondant.e, tu peux vérifier ses signatures numériques

L'idée par la suite est de faire les configurations sur Tails pour que Thunderbird gère le chiffrement de bout en bout. Pour démarrer Thunderbird choisis `Applications ▸ Internet ▸ Messagerie Thunderbird`.

▪ Configurer un compte de messagerie électronique

Lorsque Thunderbird démarre pour la première fois, un assistant apparaît pour te guider à travers le processus de configuration de Thunderbird permettant d'accéder à ton compte de courrier électronique.



Si tu n'as pas cet assistant directement, tu peux le démarrer à nouveau, depuis la fenêtre principale Thunderbird, choisir en haut à droite `Trois petits traits` ☰ `▸ Paramètres des comptes` et ensuite depuis la fenêtre `Paramètres des comptes` choisir `Gestion des comptes ▸ Ajouter un compte de messagerie…`

Dans l'assistant, entre les champs *nom*, *adresse électronique* et *mot de passe* (celui de ton e-mail). Tu dois préciser quel protocole utiliser pour se connecter à ton fournisseur de courrier électronique, soit IMAP, soit POP. Si tu sais pas trop, utilise IMAP mis par défaut.

▪ Tableau récapitulatif des différences entre pop et imap

Fait par riseup.net	POP	IMAP
Stockage	**Ton ordinateur**. En utilisant POP, tu télécharges tous tes courriels sur ton ordinateur et les supprime des serveurs de riseup.net. C'est à toi de gérer l'archivage des mails.	**Serveur Riseup**. IMAP laisse tous les messages sur le serveur. Une autre façon de voir cela est que le client courriel IMAP fournit une vue des données existantes stockées sur le serveur.
Mobilité	**Basse**. POP marche bien uniquement quand tu vérifies tes courriels principalement depuis le même ordinateur.	**Haute**. IMAP te permet d'utiliser différents clients et de les garder synchronisés.
Vitesse	**Plus rapide**, puisque tout est simplement téléchargé une fois sur ton ordinateur.	**Plus lent**, puisque le client courriel doit faire des requêtes au serveur de façon répété.

▪ Configurer une bonne phrase de passe

Il est recommandé un mot de passe long (vingtaine de caractères / 4 ou 5 mots) qui ne soit pas une citation, plutôt qu'un mot de passe court même avec des caractères compliqués. **Chaque personne détient sa façon de retenir ses phrases de passe**. Des physionomistes vont se souvenir d'un tableau dans lequel y a des éléments dedans, d'autres vont coller le tout début d'une musique qui finit par une autre, d'autres peuvent prendre 5 mots aléatoirement dans un livre, d'autres mélanger des langues.

A toi de voir ta technique, attention à la sauvegarde de mot de passe écrite à la main ou sur un document texte qui traîne et que t'oublies ! Il est recommandé quand tu commences une nouvelle phrase de passe de le taper régulièrement les premières semaines pour que ça s'ancre.

Il est ***important de ne pas utiliser le même mot de passe pour des services différents***, ça évite de tout compromettre. Le niveau de sécurité n'est pas forcément le même entre logiciels. Sur internet, on ne peut pas faire confiance aux sites internets par lesquels on passe, si tu tapes un mdp sur un site internet, il faut partir du principe que l'entreprise du site y a accès et peut analyser comment tu construits ton mdp. Régulièrement on entend tel gros serveur qui a été hacké et des millions de mdp récupérés. Il existe aussi des coffres forts à phrase de passe, c'est un outil sécurisé qui garde tes mdp. Par exemple **Kee*PassXC*** (explication de l'outil plus loin dans ce document).

> Installer une clé Tails (à partir d'une clé Tails)

Il te faut une clé usb avec déjà Tails installé. C'est la version de Tails qu'il y a sur cette clé qui sera installé sur la nouvelle clé. Attention, si le système Tails de la clé source est vérolé, la clé Tails cible le sera également ; cette manipulation est donc à faire à partir d'une clé Tails de confiance.

Une autre clé usb de plus de 8 Go[6], **attention elle sera formatée et toutes les données y seront supprimées**. S'il y avait des données auparavant sur cette clé usb, tu peux avoir envie qu'elles ne soient pas retrouvables à posteriori, il peut être intéressant d'écraser plus correctement les données avant (cf chapitre suivant)



T'allumes ta clé Tails (avec ou sans persistance ça n'a pas d'importance). Tu vas dans `Applications ▸ Tails ▸ Programme d'installation`.

Si l'installeur de Tails voit une autre clé usb, elle va être mise en « clé USB cible ».

T'as juste à faire ***Installation***, ça prend 5 à 20 min. Ta persistance ne sera pas clonée.

Si ça ne marche pas essaye de formater toi-même ta clé usb, de l'enlever / remettre et de relancer l'installation (voir le chapitre « Je n'arrive pas à installer Tails sur une clé usb »).

▪ Éviter d'avoir une clé vérolée

Une clé Tails vérolée, est une clé qui n'est pas le Tails d'origine (donc potentiellement avec des mouchards). D'autant plus si tu diffuses souvent d'autres clés Tails :

1) Évite de laisser traîner n'importe où ta clé (surtout dans les lieux surveillés), comme tu vois ça met 10 min à cloner, on pourrait très bien te cloner une autre version qui ressemblerait à Tails mais avec d'autres choses dedans comme des sniffeurs à mot de passe.

2) Ne branche jamais ta clé dans un ordi allumé. Sauf si c'est Tails qui y est allumé.

3) Fais gaffe aux clés qui peuvent revenir des perquisitions.

> Mettre à jour une clé Tails

La sécurité sur Tails (et de manière plus générale sur linux), passe par le fait que le système d'exploitation continue à être développé et que des mises à jour viennent trouver des solutions aux failles de sécurité apparaissant. La sécurité informatique d'aujourd'hui

6 Si tu peux choisir ta clé, tu peux consulter avant la liste des clés usb problématiques avec Tails pour ne pas tomber dessus : https://Tails.boum.org/support/known_issues/index.fr.html#index1h2

> Chiffrer ses mails (avec Thunderbird)

Nécessite d'avoir activé Thunderbird dans sa persistance

Note : cette méthode est intéressante sur Tails, mais est fortement déconseillée sur un système d'exploitation non chiffré, car tous les mails seraient stockés dessus, et tes clefs privée seraient accessible sans le chiffrement du système d'exploitation. S'il est possible de mettre un mot de passe principal sur thunderbird pour protéger tes mails chiffrés, il a une qualité de chiffrement plus faible. La fonction OpenPGP de Thunderbird est récente, début 2019 ça fonctionnait différemment.

Si tu veux une vulgarisation de ce qu'est **PGP et le chiffrement,** tu peux consulter l'article: « Une présentation approfondie du chiffrement de bout en bout : comment les systèmes de chiffrement à clé publique fonctionnent-ils ? » du site **Surveillance self défense**. Tu peux aussi consulter *Que devrais-je savoir au sujet du chiffrement ?* Sur le même site au sujet des différents types de chiffrements existants.

▪ Quelques explications de OpenPGP

Le chiffrement de bout en bout (end-to-end encryption) pour le courrier électronique peut être utilisé pour s'assurer que seuls l'expéditeur et les destinataires d'un message peuvent en lire les contenus. Sans cette protection, il peut être facile aux personnes administrant le réseau, aux fournisseurs de messagerie et aux agences gouvernementales de lire vos messages. Mettre en œuvre le chiffrement de bout en bout demande de l'attention à la fois à l'expéditeur.ice et aux destinatairices. Une seule erreur par une quelconque des parties impliquées peut suffire à compromettre la sécurité du chiffrement. Les métadonnées des messages électroniques ne peuvent être protégées par l'emploi du chiffrement de bout en bout. Ce sont par exemple les noms et les adresses de l'expéditeur et des destinataires, la date et l'heure auxquelles le message a été expédié, ou de quel ordinateur les messages ont été envoyés ou reçus. L'objet du message peut aussi rester non protégé et facilement lisible, même quand le chiffrement de bout en bout est utilisé.[8]

- ta **clé privée** est une donnée extrêmement sensible. Quiconque réussi à obtenir une copie de cette clé sera capable, avec le mot de passe, de lire du contenu chiffré qui n'était destiné qu'à toi uniquement. Il pourrait aussi signer des messages *à ta place*. Tu utiliseras ta *clé privée* pour déchiffrer des messages qui te sont envoyés par celleux qui ont une copie de ta *clé publique*.
- ta **clé publique** est faite pour être partagée avec les autres et ne peut être utilisée pour lire un message chiffré ou contrefaire un message. Une fois que tu as la clé publique de ton/ta correspondant.e, tu peux commencer à lui envoyer des messages chiffrés. Elle seule sera capable de déchiffrer et lire ces messages parce qu'elle seule a accès à la *clé privée* qui correspond à la *clé publique* que tu utilises pour les coder. De la même façon, pour que quelqu'un.e t'envoie un message chiffré, cette personne doit avoir une copie de ta *clé publique*. Il est important de vérifier que la *clé publique* que tu utilises pour chiffrer les messages appartient effectivement à la personne avec qui tu essayes d'échanger (à partir de l'empreinte numérique de la clé). Si toi ou ton/ta correspondant.e êtes dupé.es lors du chiffrement des messages avec la mauvaise clé publique, votre conversation ne sera pas sécurisée.

8 Plus d'informations sur la page « Présentation du chiffrement de bout en bout dans Thunderbird » de support.mozilla.org ou encore sur « OpenPGP dans Thunderbird – Guide et questions fréquentes ».

est bien complet. Il existe pour cela « GTKhash ». C'est ce qu'on appelle « vérifier les sommes de contrôle (MD5, SHA1, SHA256) ». Cela permet de vérifier sur le document téléchargé que tu as la même somme de contrôle que la personne qui l'a mise sur le site, ainsi sur le site s'il y a la somme de contrôle SHA256, il suffit de le copier dans « vérifier », mettre le fichier télécharger, le « hacher » (opération qui ne peut pas altérer le fichier). En terme de vérification : *SHA256 > SHA1 > MD5*. Si y a le point vert, c'est que le fichier n'a pas été altéré pendant le téléchargement.

2) Vérifier l'origine du fichier

Pour être sûr que le fichier que tu viens de télécharger appartienne bien à X et pas à un intermédiaire Y, une possibilité de vérification par pgp existe, pour cela il faut que X ait *signé* son document et ait laissé la possibilité d'accéder à sa clé publique.

Pour cela il faut utiliser le logiciel Kleopatra.

3) Notion de confiance

Malgré tout ça, se pose la question de la confiance qu'on peut avoir dans le groupe qui gère le fichier téléchargé : fait-il bien ce qu'il dit ? (attention aux véreux.ses qui traînent sur internet). Cela repose souvent sur ce qu'on appelle une toile de confiance.
S'il y a risque, en fonction du modèle de menace, une solution est de télécharger un fichier avec une clé Tails, de ne pas l'ouvrir et avoir par exemple une 2e clé Tails que t'allumes en désactivant internet. Pour cela au démarrage, sur la page de mot de passe de persistance tu fais le petit + en bas, et tu peux mettre une option sans accès à internet. Et là seulement t'ouvres le document.

> Installer des logiciels additionnels

Attention : Si t'installes des nouveaux logiciels, c'est à toi de vérifier qu'il n'y a pas de faille de sécurité, et de le configurer pour passer par Tor s'il passe par internet. Si les logiciels utilisés dans Tails sont audités en terme de sécurité ça ne sera pas forcément le cas pour ce que tu installeras. Avant d'installer un nouveau logiciel, c'est mieux de vérifier qu'il n'y a pas déjà un logiciel dans Tails qui fait déjà le taf que tu souhaites faire. Ici on va voir comment installer un logiciel parmi les *paquets* de Debian.

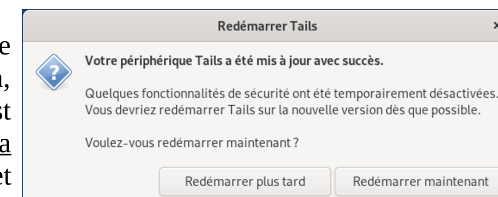
En prérequis il faut que t'aies coché « logiciels additionnels » dans la configuration de ta persistance (cf chapitre associé). Il te faut démarrer Tails avec des droits d'administrateurices (cf chapitre associé), aller dans *applications ▸ outil système ▸ gestionnaire de paquets synaptic*. Là tu mets ton mot de passe admin (si c'est la première fois que tu fais ça, ça va prendre du temps pour télécharger les dépots). Tu vas dans « Toutes » et tu choisis le logiciel que tu souhaites installer « sélectionner pour installation » puis « appliquer ». Une fois fait, Tails te demandera, si ta persistance est ouverte, si tu veux l'installer une fois, où l'ajouter à ta persistance. Si tu l'ajoute à la persistance, les paquets logiciels correspondants sont stockés dans le stockage persistant. Ils sont automatiquement mis à jour par sécurité dès qu'une connexion réseau est établie. Tu pourras accéder aux logiciels additionnels que t'as installés pour éventuellement les supprimer dans *Applications ▸ outils système ▸ logiciels additionnels*.

Plus d'informations dans la documentation Tails : '*Installer des logiciels supplémentaires*'.

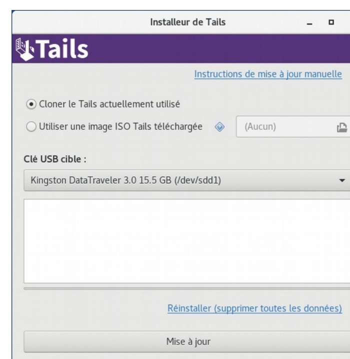
sera obsolète dans 5 ans. Il est très important de **faire les mises à jour régulièrement** (Tails en fait une par mois). Les mises à jour correspondent à la mise à jour de Tails, et de tous les logiciels qui y sont utilisés (debian, Tor, thunderbird, …), ils permettent aussi de fixer des bugs, mais parfois de nouveaux peuvent apparaître (surtout sur les gros changements).

Il existe 2 types de mises à jour, t'en seras informé·e par un mot quand tu te connectes à internet, lis le bien :

1) La mise à jour automatique.



T'as juste à lancer le téléchargement. Il faut se prévoir un peu de temps et bien attendre la fin, un moment ça va couper ton internet, c'est normal ! Mais surtout, il faut bien attendre la fenêtre *Redémarrer Tails*, avant d'éteindre (et pas avant). S'il y a un bug (extinction avant la fin), tes données ne sont pas affectées par la mise à jour, mais tu risques de pas pouvoir redémarrer sur ta clef Tails.…



2) La mise à jour manuelle

- Si t'as déjà une clé Tails avec la dernière version, tu démarres sur celle là, et comme pour l'installation *Applications ▸ Tails ▸ Programme d'installation*. Sauf que là, plutôt que de mettre « installation », on va te demander « mettre à jour », la différence c'est que ça ne formatera pas toute la clé usb, ça remplacera juste la partition de la Tails allumée par celle qui est mise à jour. (tu peux donc mettre à jour d'autres personnes, attention aux clés Tails vérolées !)
- Si tu ne connais personne, il te faudra une clé USB vierge ou une autre clé Tails (donc pas à jour), et tu pourras télécharger ce qu'il te faut en suivant le tuto Tails qui te suit pas à pas : *https://Tails.boum.org/upgrade/index.fr.html*

=> ce type de mise à jour n'a lieu que pour les mises à jour majeurs ou en cas de bug.

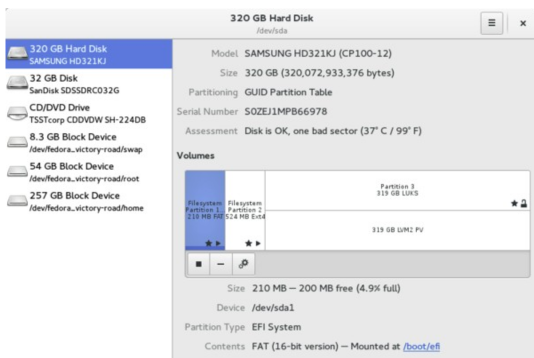
II) Pour aller plus loin :
quelques trucs et astuces supplémentaires

> Supprimer vraiment des données d'une clé usb

« **Supprimer de manière définitive** » ou « **mettre à la corbeille** » ne supprime pas les données. … et ça peut être très facile de les retrouver. En effet, lorsqu'on « supprime » un fichier — en le plaçant dans la *Corbeille* puis en la vidant — on ne fait que dire au système d'exploitation que le contenu de ce fichier ne nous intéresse plus. Il supprime alors son entrée dans l'index des fichiers existants. Il a ensuite le loisir de réutiliser l'espace que prenaient ces données pour y inscrire autre chose.

Mais il faudra peut-être des semaines ou des années avant que cet espace soit *effectivement* utilisé pour de nouveaux fichiers, et que les anciennes données disparaissent réellement. En attendant, si on regarde directement ce qui est inscrit sur le disque dur, on retrouve le contenu des fichiers. C'est une manipulation assez simple, automatisée par de nombreux logiciels permettant de « récupérer » ou de « restaurer » des données. On ne peut pas réellement supprimer des données en informatique, cependant on peut « **réécrire des données par dessus** ». Il peut rester cependant des traces des données inscrites auparavant, notamment en cas d'accès physique au matériel. Attention si sur ta clé usb ou sur ton disque dur tu as des documents sensibles à supprimer vraiment, il vaut mieux se référer à l'article : *Effacer des données « pour de vrai »* sur le *guide d'autodéfense numérique*[7]. Pour des données très sensibles il n'existe pas 100 % d'assurance de ne retrouver aucune trace, s'il y en a l'occasion il est préférable de les mettre sur un support chiffré auparavant.

Sur Tails, tu peux faire clic droit sur un fichier, **écraser les données** (par défaut ça fait 2 passes, c'est-à-dire réécris des données 2 fois à la place du fichier à écraser), *attention si c'est un fichier très gros ça va prendre du temps*. Cette opération va supprimer les données là où se trouve le fichier, mais il est possible qu'il y ait une partie des données qui ait pu être enregistré ailleurs sur le support. Pour écraser l'ensemble d'une clé usb, tu peux quand tu la formates faire « écraser les données existantes avec des zéros » (le faire 2 fois peut être une bonne idée).



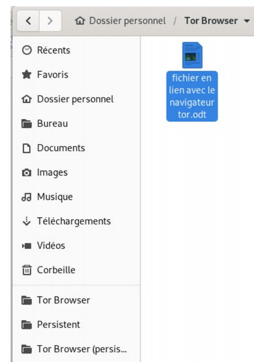
> Comment créer un disque dur ou une clé usb chiffrée (ouvrable sur des linux)

Dans Tails tu peux aller dans `Applications ▸ Utilitaires ▸ Disques`. Là **tu sélectionnes le bon disque** (c'est à dire ta clé usb ou ton disque dur, attention de ne pas se tromper !), tu formates tout le disque ainsi que ses

7 https://guide.boum.org/tomes/1_hors_connexions/3_outils/06_effacer_pour_de_vrai/

t'auras à choisir le bon. **Tu dois faire très attention à ne pas te tromper d'icônes. De même s'il y a un nom d'utilisateur.ice + un mdp à mettre dans ta fenêtre, vérifie avant qu'il y ait les 2 indiqués dans l'entrée que tu vas auto-remplir. S'il n'y a qu'un mdp, il sera envoyé dans le nom d'utilisateur.ice.**

> Téléchargement / téléversement et le dossier Tor browser



Une protection sur Tails existe qui fait que le navigateur Tor n'a pas accès à vos dossiers (persistance, clés usb ou tout autre), ça évite qu'il fouine dans vos documents, ce qu'on appelle un ***bac à sable***. Pour télécharger il faut donc télécharger dans le dossier *Tor Browser* puis mettre ensuite dans le dossier que vous souhaitez / dans la persistance. De la même manière, si vous voulez téléverser un document (= le mettre sur internet, l'envoyer sur un site ou en pj), il faut d'abord le copier dans le dossier *Tor Browser* avant de le téléverser.

▪ Peu de RAM ou téléchargement de gros fichiers

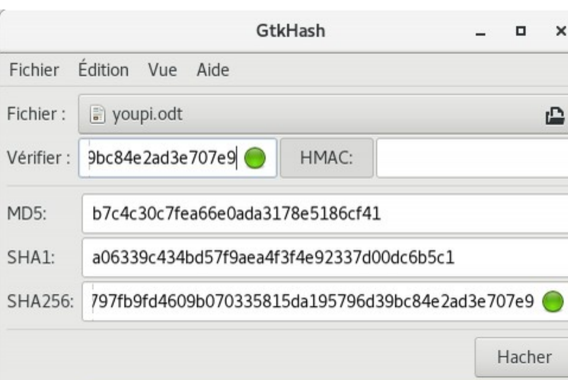
Il existe deux dossiers Tor Browser, un qui n'est pas persistant, l'autre qui l'est (qui s'allume que si tu as activé la persistance au démarrage). Celui qui n'est pas persistant enregistre dans la RAM. Attention donc si tu télécharges trop dessus ça va ralentir la clé Tails. De manière générale si trop de documents / trop d'onglets sont ouverts ou si trop de documents sont enregistrés sur autre chose que la persistance ça peut faire buguer ou ralentir. Si tu as donc un gros téléchargement vaut mieux le faire dans le dossier Tor Browser persistant. Mais ne laisse pas tout tes documents dedans si tu veux que le bac à sable soit efficace.

▪ Format de fichier HTML

Les fichiers en html ne peuvent pas être ouverts sur la persistance, il faut donc les mettre dans le dossier Tor Browser avec le dossier de configuration (pour avoir les images) avant de l'ouvrir. Tu n'auras pas besoin d'internet pour l'ouvrir.

▪ Document téléchargé et vérifications

Avisé. Prérequis : connaître pgp, ce qu'est une signature de document et une clef publique



Les fichiers téléchargés sur internet peuvent être dangereux, car possédant possiblement des logiciels malveillants. En fonction de ton modèle de menace / de la sensibilité / du type de document il peut s'avérer nécessaire de prendre plusieurs précaution :

1) Vérifier l'intégrité d'un document (important pour les logiciels / images iso), vérifier que ce qu'on a téléchargé

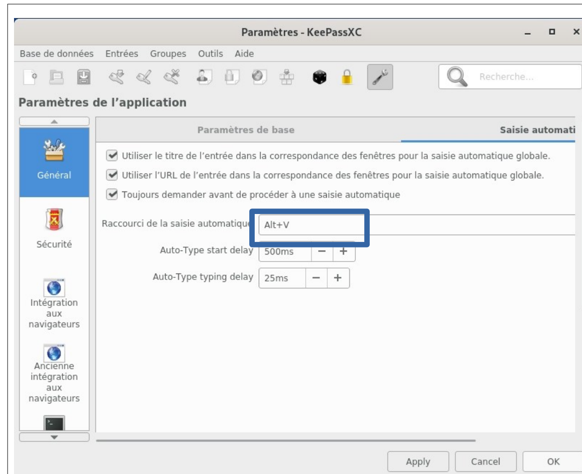
▪ **Rendre persistent les paramétrages de KeepassXC**

Pour faire en sorte que tes paramètres de KeePassXC soit persistent, il faut que « Dotfiles » soit activé (dans `Applications ▸ Tails ▸ Configurer le stockage…`). Tu vas dans le `Dossier personnel`, en activant les fichiers cachés (ctrl+h). Dans `.config` tu copies le dossier `KeePassXC`. Tu le colles dans un dossier s'appelant exactement `.config` que tu créés dans `Emplacements ▸ dotfiles`.
Tu peux maintenant par exemple **changer le délais de verrouillage de KeePassXC** dans `outil ▸ paramètres ▸ Sécurité ▸ Verrouiller les bases de données après une inactivité de [ton_temps]`.

▪ **Utiliser les paramètres de remplissage automatique de KeePassXC**

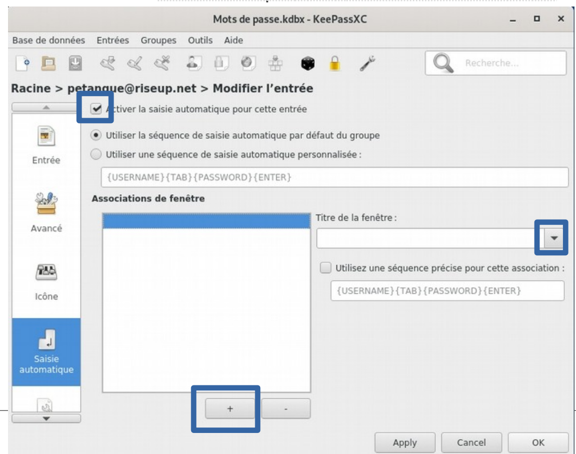
Bonus - gestion mdp - sensible

A utiliser avec prudence et s'expérimenter sur cette fonction avant, **une erreur de manipulation peut entraîner l'envoie de mots de passe dans de mauvaises mains. Par exemple l'auto-remplissage se faisant avec un nom de fenêtre, dans cette fenêtre il peut y avoir plusieurs cases à remplir. Ainsi si tu mets le navigateur Tor comme nom de fenêtre à auto-remplir, et que tu fais l'opération dans l'URL, ton moteur de recherche va récupérer en clair ton mdp.**



1) Configurer les touches qui feront le remplissage automatique
Dans KeePassXC faire (en haut) `outil ▸ paramètres ▸ mettre les touches qu'on veut dans « raccourci de remplissage automatique global »` (genre alt+v par exemple, pas de raccourcis utilisés par d'autres fonctions comme Ctr+c). **Ce paramètre ne s'enregistre pas de manière persistante par défaut** (cf partie au dessus).

2) Configurer le remplissage automatique de l'entrée
Revenir dans la fenêtre des mots de passe de KeePassXC. Faire `clic droit sur l'entrée souhaitée ▸ Voir/Editer l'entrée ▸ à gauche « Saisie automatique » ▸ en bas le « + »` et rajouter le titre de la fenêtre. Pour cela, regarder le nom de la fenêtre qui s'ouvre pour demander un mot de passe, et soit la taper dans le titre précédemment dit, soit si cette fenêtre du mot de passe est ouverte en parallèle du KeePassXC il suffit de cocher la petite flèche à droite du titre de la fenêtre et de choisir le bon nom de fenêtre.



3) Effectuer le remplissage automatique
Dans la fenêtre qui demande le mot de passe, tu appuies sur les touches choisies dans ***1)***. S'il y a plusieurs mots de passe qui ont le même nom de remplissage

partitions en faisant les `3 petits traits en haut à droite de l'écran ≡ ▸ Formater le disque`. Quand c'est fini il n'y a plus rien du tout sur ton disque, tu cliques sur le « + », tu choisis la taille de ta partition (tout si tu n'en veux qu'une), « suivant », dans `« type » ▸ « disque interne à utiliser avec les systèmes Linux uniquement (Ext4) »` (= tu ne pourras pas aller sur cette clé avec windows et mac), tu coches « Volume protégé par mot de passe (LUKS) », par la suite t'auras à mettre un mot de passe (à cette occasion tu peux décider de faire « écraser les données existantes, mais prend plus de temps », s'il y a des documents sensibles, cf chapitre S*upprimer vraiment des données*). Comme tu le vois c'est possible de recréer un `type « Fat »` pour avoir une clé usb consultable sur tout système d'exploitation (ou presque).

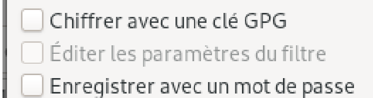
> Chiffrer un fichier / un document par une phrase de passe – ou par une clé publique

▪ **Sur un fichier de manière générale**

Dans Tails tu peux très bien faire *clic droit* sur un fichier, faire « **chiffrer** » choisir « ***use passphrase only*** » ou par clé publique. Ça va créer un fichier en .pgp. Attention à supprimer les données non chiffrées pour de vrai après coup (cf chapitre au dessus).

Si tu choisis l'option **passphrase**, il faudra ouvrir le fichier dans Tails et taper la phrase de passe. Si tu ne veux pas que les données non chiffrées soient marquées à l'emplacement où tu l'ouvres (par exemple sur une clé usb), il vaut mieux d'abord copier le fichier chiffré dans un dossier Tails qui est uniquement en mémoire vive (par exemple `Emplacements ▸ Documents`) avant de l'ouvrir.

▪ **Sur un document *Libre Office***



Lorsque tu sauvegardes ton fichier la première fois, il te demande dans quel dossier tu veux le sauvegarder, en bas à gauche tu peux cocher sur la case « *enregistrer avec un mot de passe* ». **Bonus** : à l'étape d'après, si tu cliques sur *options*, tu peux même décider de mettre un mdp d'édition.

> S'ajouter des droits d'administrateurices

Dans Tails, un mot de passe d'administration (également appelé *mot de passe root* ou *mot de passe amnesia*) est nécessaire pour effectuer des tâches d'administration système. Par exemple :

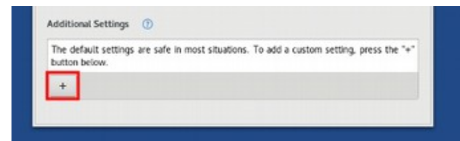
- Pour installer des logiciels additionnels
- Pour accéder aux disques durs internes de l'ordinateur
- Pour lancer des commandes en *terminal superutilisateur.ice*.
- Pour accéder à certains droits, notamment quand t'as une fenêtre qui demande une authentification avec écrit *administrateur* en orange.

Par défaut, le mot de passe d'administration est désactivé pour plus de sécurité. Ce qui peut empêcher un.e attaquant.e ayant un accès physique ou à distance à ton système Tails d'obtenir les droits d'administration et d'effectuer des tâches d'administration contre ta

volonté. De même, si tu te mets un mot de passe admin, tu te donnes la possibilité d’atterrer la sécurité de Tails.

▪ Définir un mot de passe d'administration

Afin d'effectuer des tâches d'administration, tu dois choisir un *mot de passe d'administration* lors du démarrage de Tails, en utilisant Tails Greeter.



1. Lorsque Tails Greeter apparaît, clique sur le bouton +.
2. Lorsque la fenêtre *Paramètres supplémentaires* apparaît, clique sur « Mot de passe d'administration ».
3. Saisis un mot de passe de ton choix dans les zones de texte « Mot de passe d'administration » et confirme puis clique sur « Ajouter ».

Ce mot de passe ne dure que durant la session. Tu peux avoir ces droits d’administration avec ou sans persistance.

> MAT2 - supprimer les métadonnées sur des fichiers

Beaucoup de fichiers que nous utilisons (images, sons, vidéos, documents texte, …) contiennent des **métadonnées.** Ce sont des données inscrites dans le fichier, mais qui ne constituent pas le contenu du fichier (un peu comme le générique d’un film). Par exemple, les métadonnées d‘une photo peuvent comporter la taille de ta photo en pixels, la marque et le modèle de ton appareil, son numéro de série … Si la photo a été prise depuis un téléphone, on peut y ajouter les coordonnées GPS du téléphone lors de la prise de vue, et de manière générale toutes les options définies dans ton téléphone (nom pré-enregistré). Et enfin le nom de ton ordi, les logiciels qui ont servi à la modifier, etc.

MAT2 (pour ***Metadata Anonymisation Toolkit 2***) est un logiciel qui permet de supprimer les métadonnées de tes fichiers. Pour ça dans Tails tu fais *clic droit* sur le fichier que tu veux nettoyer puis « *remove metadata* », un fichier sans métadonnées personnelles sera créé juste à côté « nom_du_fichier.cleaned ». Tu l’ouvres pour vérifier que tout est bon dedans puis tu supprimes l’ancien fichier (voir le chapitre *Supprimer vraiment des données*). **Si le fichier .cleaned n’a pas été créé c’est que mat2 n’a pas marché.** Certains formats de fichiers ne fonctionnent pas avec Mat2 (tu peux voir la liste en ouvrant un terminal et en écrivant « mat2 -l »). Sur la version actuelle sont prises en compte :

Application *: .epub, .pdf, .odc, .odf, .odg, .odi, .odp, .ods, .odt, .pptx, .xlsx, .docx, .torrent, .ncx, .zip,**audio** : .flac, .mpega, .mpga, .mp1, .mp2, .mp3, .m4a, .opus, .oga, .ogg, .spx, .wav,* ***image*** *: .gif, .jpg, .jpeg, .jpe, .png, .svg, .svgz, .tiff, .tif, .bmp, .ppm, .jfif,* ***texte*** *: .css, .htm, .shtml, .html, .text, .txt,* ***vidéo*** *: .mp4, .m4v, .mp4, .mpg4, .xmv, .avi.*

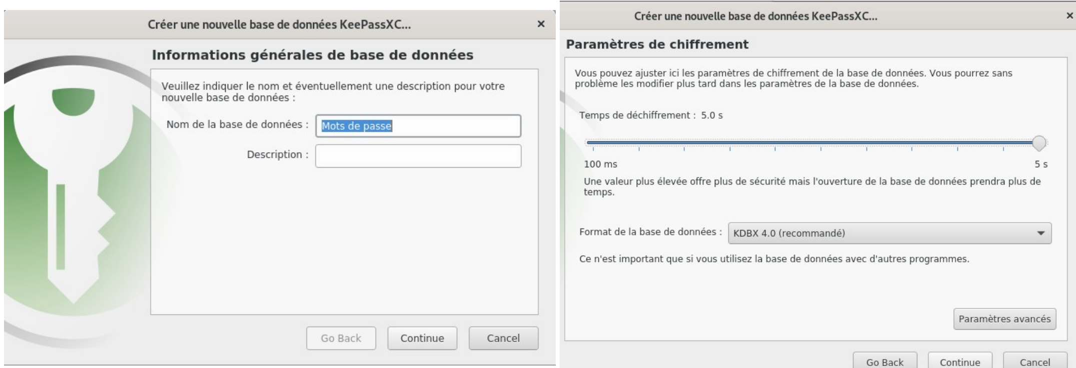
▪ Cas du pdf :

Pour les *pdf* (format de fichier compliqué), **il vaut mieux effacer les métadonnées du fichier texte** avant de le convertir en pdf sur Tails. Si tu n’as que la version pdf, quand tu vas faire « remove metadata », Mat2 va d’abord le transformer en image, supprimer les

métadonnées et le remettre en pdf. L’inconvénient, c’est que tu ne pourras plus sélectionner le texte, tu vas perdre en qualité et le document risque d’être plus lourd.
Il est possible de supprimer une partie des métadonnées du pdf sans le dégrader, en ligne de commande. Pour cela tu ouvres `Application ▸ Utilitaires ▸ Terminal` et tu tappes :
mat2 –L [chemin_du_fichier]
Pour avoir le chemin du fichier, tu peux « glisser » ton pdf dans le terminal. Attention si ton fichier est sensible, certaines métadonnées ne seront pas supprimés par ce processus.

> Coffre fort à mot de passe (KeePassXC)

Si tu es amené·e à devoir connaître beaucoup de mots de passe, il peut être bien d’avoir un moyen sécurisé de les stocker (et pas un bout de papier à côté de ton ordi).
Il existe `KeePassXC (Application ▸ Favoris ▸ KeePassXC)`.



Lorsque tu fais une nouvelle base de données, dans les impressions d’écran au dessus tu peux retrouver les différentes étapes pour faire ta clef. A la fin il t’est proposé de mettre ton mot de passe principal qui va protéger ton coffre fort à mot de passe puis de sauvegarder ton fichier KeePassXC qu’il faut mettre dans ton persistent. C’est ce fichier qui comportera tous tes mots de passe.

Dès que tu fermes KeePassXC ou si tu ne l’utilises pas quelques minutes il se chiffre. Attention à ne pas oublier ta phrase de passe principale.

